



Informatica®  
10.5.2

# Befehlsreferenz

Diese Software und die Dokumentation werden nur im Rahmen eines eigenen Lizenzvertrags zur Verfügung gestellt, der Beschränkungen für die Verwendung und Weitergabe enthält. Ohne ausdrückliche schriftliche Genehmigung der Informatica LLC darf kein Teil dieses Dokuments zu irgendeinem Zweck vervielfältigt oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen usw.) dies geschieht.

Informatica, das Informatica-Logo, PowerCenter, PowerExchange, Big Data Management und Enterprise Data Catalog sind Marken oder eingetragene Marken der Informatica LLC in den Vereinigten Staaten von Amerika und zahlreichen anderen Ländern der Welt. Eine aktuelle Liste der Informatica-Marken ist im Internet auf <https://www.informatica.com/trademarks.html> verfügbar. Alle weiteren Produkt- und Firmennamen sind möglicherweise Markennamen oder Warenzeichen der jeweiligen Eigentümer.

Gemäß Ihren Opt-out-Rechten überträgt die Software automatisch Informationen über die Computer- und Netzwerkumgebung, in der die Software bereitgestellt wird, sowie über die Datennutzung und Systemstatistiken der Bereitstellung an Informatica in den USA. Diese Übertragung gilt als Teil der Services/Dienste im Rahmen der Datenschutzrichtlinie von Informatica; die Verwendung und anderweitige Verarbeitung der Informationen durch Informatica erfolgen entsprechend der Datenschutzrichtlinie von Informatica, die hier zur Verfügung steht: <https://www.informatica.com/in/privacy-policy.html> Sie können die Sammlung von Nutzungsdaten im Administrator-Tool deaktivieren.

Den RECHTEN DER REGIERUNG DER VEREINIGTEN STAATEN unterliegende Programme, Software, Datenbanken und zugehörige Dokumentation und technische Daten, die an Kunden der Regierung der Vereinigten Staaten geliefert werden, sind "kommerzielle Computersoftware" oder "kommerzielle technische Daten" gemäß der anwendbaren Beschaffungsverordnung der Vereinigten Staaten (Federal Acquisition Regulation – FAR) und der ergänzenden Bestimmungen der spezifischen Behörde. Damit unterliegen die Nutzung, das Kopieren, die Offenlegung, das Modifizieren und die Anpassung den im anwendbaren Regierungsvertrag gemachten Einschränkungen und Lizenzbedingungen und, soweit im Rahmen der Bedingungen des Regierungsvertrags und der in FAR 52.227-19 aufgeführten Rechte anwendbar, der Lizenz für die kommerzielle Computersoftware.

Teile dieser Software und/oder Dokumentationen unterliegen dem Urheberrecht Dritter. Die erforderlichen Hinweise auf Drittanbieter sind im Lieferumfang des Produkts enthalten.

Weitere Informationen über die Patente finden Sie unter <https://www.informatica.com/legal/patents.html>.

Die in dieser Dokumentation enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden. Wenn Sie Probleme in dieser Dokumentation finden, melden Sie sie uns unter [infa\\_documentation@Informatica.com](mailto:infa_documentation@Informatica.com).

Informatica-Produkte unterliegen einer Gewährleistung gemäß den Geschäftsbedingungen der Vereinbarungen, unter denen sie bereitgestellt werden. INFORMATICA STELLT DIE INFORMATIONEN IN DIESEM DOKUMENT OHNE MÄNGELGEWÄHR UND OHNE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNG JEGLICHER ART ZUR VERFÜGUNG. DIES GILT EINSCHLIESSLICH FÜR GEWÄHRLEISTUNGEN DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND GEWÄHRLEISTUNGEN ODER ZUSICHERUNGEN ÜBER DIE NICHTVERLETZUNG VON RECHTEN DRITTER.

# Inhalt

<b>Einleitung .....</b>	<b>27</b>
Informatica-Ressourcen. ....	27
Informatica Network. ....	27
Informatica-Wissensdatenbank. ....	27
Informatica-Dokumentation. ....	28
Informatica-Produktverfügbarkeitsmatrizen. ....	28
Informatica Velocity. ....	28
Informatica Marketplace. ....	28
Globaler Kundensupport von Informatica. ....	28
 <b>Kapitel 1: Befehlszeilenprogramme und Dienstprogramme.....</b>	<b>29</b>
Befehlszeilenprogramme und Dienstprogramme - Übersicht. ....	29
 <b>Kapitel 2: Installieren und Konfigurieren von Befehlszeilendienstprogrammen.....</b>	<b>31</b>
Installieren und Konfigurieren von Befehlszeilendienstprogrammen – Übersicht. ....	31
Installieren der Befehlszeilendienstprogramme. ....	32
Installationsverzeichnisse. ....	32
Konfigurieren der Befehlszeilendienstprogramme. ....	33
Konfigurieren der Informatica-Dienstprogramme. ....	33
Konfigurieren der PowerCenter-Dienstprogramme. ....	33
Konfigurieren der Metadata Manager-Dienstprogramme. ....	34
Erstellen der Datei „domains.infa“. ....	34
Sicherheitskonfiguration für Informatica-Dienstprogramme. ....	35
 <b>Kapitel 3: Verwenden der Befehlszeilenprogramme.....</b>	<b>36</b>
Verwenden der Befehlszeilenprogramme - Übersicht. ....	36
Eingeben von Optionen und Argumenten. ....	37
Syntax-Notation. ....	38
Ausführen von Befehlen in einer sicheren Domäne. ....	39
Ausführen von Befehlen unter UNIX mit Kerberos-Authentifizierung. ....	40
Ausführen von Befehlen unter UNIX mit Single Sign On. ....	40
Ausführen von Befehlen unter UNIX ohne Single Sign On. ....	41
Ausführen von Befehlen unter Windows mit Kerberos-Authentifizierung. ....	41
 <b>Kapitel 4: Umgebungsvariablen für Befehlszeilenprogramme.....</b>	<b>43</b>
Umgebungsvariablen für Befehlszeilenprogramme - Übersicht. ....	44
ICMD_JAVA_OPTS. ....	45
Konfigurieren von ICMD_JAVA_OPTS unter UNIX. ....	46
Konfigurieren von ICMD_JAVA_OPTS unter Windows. ....	46

INFA_CLIENT_RESILIENCE_TIMEOUT. . . . .	46
Konfigurieren von INFA_CLIENT_RESILIENCE_TIMEOUT unter UNIX. . . . .	46
Konfigurieren von INFA_CLIENT_RESILIENCE_TIMEOUT unter Windows. . . . .	47
INFA_CODEPAGENAME. . . . .	47
Konfigurieren von INFA_CODEPAGENAME unter UNIX. . . . .	47
Konfigurieren von INFA_CODEPAGENAME unter Windows. . . . .	47
INFA_DEFAULT_DATABASE_PASSWORD. . . . .	47
Konfigurieren von INFA_DEFAULT_DATABASE_PASSWORD unter UNIX. . . . .	48
Konfigurieren von INFA_DEFAULT_DATABASE_PASSWORD unter Windows. . . . .	48
INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD. . . . .	49
Konfigurieren von INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD unter UNIX. . . . .	49
Konfigurieren von INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD unter Windows. . . . .	49
INFA_DEFAULT_DOMAIN. . . . .	50
Konfigurieren von INFA_DEFAULT_DOMAIN unter UNIX. . . . .	50
Konfigurieren von INFA_DEFAULT_DOMAIN unter Windows. . . . .	50
INFA_DEFAULT_DOMAIN_PASSWORD. . . . .	50
Konfigurieren von INFA_DEFAULT_DOMAIN_PASSWORD unter UNIX. . . . .	51
Konfigurieren von INFA_DEFAULT_DOMAIN_PASSWORD unter Windows. . . . .	51
INFA_DEFAULT_DOMAIN_USER. . . . .	51
Konfigurieren von INFA_DEFAULT_DOMAIN_USER unter UNIX. . . . .	51
Konfigurieren von INFA_DEFAULT_DOMAIN_USER unter Windows. . . . .	52
INFA_DEFAULT_PWX_OSEPASSWORD. . . . .	52
Konfigurieren von INFA_DEFAULT_PWX_OSEPASSWORD unter UNIX. . . . .	52
Konfigurieren von INFA_DEFAULT_PWX_OSEPASSWORD unter Windows. . . . .	53
INFA_DEFAULT_PWX_OSPASSWORD. . . . .	53
Konfigurieren von INFA_DEFAULT_PWX_OSPASSWORD unter UNIX. . . . .	53
Konfigurieren von INFA_DEFAULT_PWX_OSPASSWORD unter Windows. . . . .	53
INFA_DEFAULT_SECURITY_DOMAIN. . . . .	53
Konfigurieren von INFA_DEFAULT_SECURITY_DOMAIN unter UNIX. . . . .	54
Konfigurieren von INFA_DEFAULT_SECURITY_DOMAIN unter Windows. . . . .	54
INFA_DOMAINS_FILE. . . . .	54
Konfigurieren von INFA_DOMAINS_FILE unter UNIX. . . . .	54
Konfigurieren von INFA_DOMAINS_FILE unter Windows. . . . .	55
INFA_JAVA_CMD_OPTS. . . . .	55
Konfigurieren von INFA_JAVA_CMD_OPTS unter UNIX. . . . .	55
Konfigurieren von INFA_JAVA_CMD_OPTS unter Windows. . . . .	55
INFA_PASSWORD. . . . .	55
Konfigurieren von INFA_PASSWORD unter UNIX. . . . .	56
Konfigurieren von INFA_PASSWORD unter Windows. . . . .	56
INFA_NODE_KEYSTORE_PASSWORD. . . . .	57
Konfigurieren von INFA_NODE_KEYSTORE_PASSWORD unter UNIX. . . . .	57
Konfigurieren von INFA_NODE_KEYSTORE_PASSWORD unter Windows. . . . .	57



INFA_NODE_TRUSTSTORE_PASSWORD. . . . .	58
Konfigurieren von INFA_NODE_TRUSTSTORE_PASSWORD unter UNIX. . . . .	58
Konfigurieren von INFA_NODE_TRUSTSTORE_PASSWORD unter Windows. . . . .	58
INFA_REPCNX_INFO. . . . .	58
Konfigurieren von INFA_REPCNX_INFO unter UNIX. . . . .	59
Konfigurieren von INFA_REPCNX_INFO unter Windows. . . . .	59
INFA_REPOSITORY_PASSWORD. . . . .	59
Konfigurieren von INFA_REPOSITORY_PASSWORD unter UNIX. . . . .	60
Konfigurieren von INFA_REPOSITORY_PASSWORD unter Windows. . . . .	60
INFATool_DATEFORMAT. . . . .	60
Konfigurieren von INFATool_DATEFORMAT unter UNIX. . . . .	60
Konfigurieren von INFATool_DATEFORMAT unter Windows. . . . .	61
Encrypting Passwords. . . . .	61
Verwenden eines Passworts als eine Umgebungsvariable. . . . .	62
Festlegen des Benutzernamens. . . . .	62
Konfigurieren eines Benutzernamens als eine Umgebungsvariable unter UNIX. . . . .	63
Konfigurieren eines Benutzernamens als eine Umgebungsvariable unter Windows. . . . .	63
<b>Kapitel 5: Verwenden von infacmd. . . . .</b>	<b>64</b>
Verwenden von infacmd - Übersicht. . . . .	64
infacmd ListPlugins. . . . .	65
Running Commands. . . . .	65
Herstellen einer Verbindung zur Domäne. . . . .	66
infacmd-Rückgabewerte. . . . .	67
<b>Kapitel 6: infacmd as-Befehlsreferenz. . . . .</b>	<b>68</b>
CreateExceptionAuditTables. . . . .	68
CreateService. . . . .	70
DeleteExceptionAuditTables. . . . .	72
ListServiceOptions. . . . .	73
ListServiceProcessOptions. . . . .	73
UpdateServiceOptions. . . . .	74
UpdateServiceProcessOptions. . . . .	75
<b>Kapitel 7: infacmd aud-Befehlsreferenz. . . . .</b>	<b>77</b>
getDomainObjectPermissions. . . . .	77
getPrivilegeAssociation. . . . .	78
getUserGroupAssociation. . . . .	80
getUserGroupAssociationForRoles. . . . .	81
getUsersPersonallInfo. . . . .	82
<b>Kapitel 8: infacmd autotune-Befehlsreferenz. . . . .</b>	<b>85</b>
Autotune. . . . .	85

## **Kapitel 9: Infacmd bg-Befehlsreferenz..... 87**

upgradeRepository. . . . .	87
deleteAuditHisotry. . . . .	88
listGlossary. . . . .	89
exportGlossary. . . . .	90
importGlossary. . . . .	92

## **Kapitel 10: infacmd ccps-Befehlsreferenz..... 95**

deleteClusters. . . . .	95
listClusters. . . . .	97
updateADLSCertificate. . . . .	99

## **Kapitel 11: infacmd cluster-Befehlsreferenz ..... 102**

createConfiguration. . . . .	102
createConfigurationWithParams. . . . .	105
deleteConfiguration. . . . .	107
clearConfigurationProperties. . . . .	109
exportConfiguration. . . . .	111
listAssociatedConnections. . . . .	113
listConfigurationGroupPermissions. . . . .	115
listConfigurationSets. . . . .	117
listConfigurationProperties. . . . .	118
listConfigurations. . . . .	120
listConfigurationUserPermissions. . . . .	122
refreshConfiguration. . . . .	123
setConfigurationPermissions. . . . .	125
setConfigurationProperties. . . . .	127
updateConfiguration. . . . .	129

## **Kapitel 12: infacmd cms-Befehlsreferenz..... 132**

CreateAuditTables. . . . .	132
CreateService. . . . .	134
DeleteAuditTables. . . . .	137
ListServiceOptions. . . . .	139
ListServiceProcessOptions. . . . .	141
Löschen. . . . .	143
RemoveService. . . . .	145
ResyncData. . . . .	147
UpdateServiceOptions. . . . .	149
UpdateServiceProcessOptions. . . . .	152
Upgrade. . . . .	154

<b>Kapitel 13: infacmd dis-Befehlsreferenz.....</b>	<b>156</b>
AddParameterSetEntries. . . . .	157
BackupApplication. . . . .	159
CancelDataObjectCacheRefresh. . . . .	161
CreateService. . . . .	163
compareMapping. . . . .	166
compareObject. . . . .	170
DeleteParameterSetEntries. . . . .	174
deployObjectsToFile. . . . .	177
DeployApplication. . . . .	181
disableMappingValidationEnvironment. . . . .	183
enableMappingValidationEnvironment. . . . .	187
ListApplicationObjectPermissions. . . . .	191
ListApplicationObjects. . . . .	193
ListApplicationOptions. . . . .	195
ListApplicationPermissions. . . . .	197
ListApplications. . . . .	199
ListComputeOptions. . . . .	200
ListDataObjectOptions. . . . .	202
ListMappingEngines. . . . .	204
ListParameterSetEntries. . . . .	207
ListParameterSetObjects. . . . .	209
ListParameterSets. . . . .	211
listPatchNames. . . . .	212
ListSequenceObjectProperties. . . . .	214
ListSequenceObjects. . . . .	216
ListServiceProcessOptions. . . . .	217
PurgeDataObjectCache. . . . .	219
PurgeResultSetCache. . . . .	221
queryDesignTimeObjects. . . . .	223
queryRunTimeObjects. . . . .	225
RefreshDataObjectCache. . . . .	227
RenameApplication. . . . .	228
replaceMappingHadoopRuntimeConnections. . . . .	230
RestoreApplication. . . . .	233
SetApplicationPermissions. . . . .	234
SetApplicationObjectPermissions. . . . .	237
setMappingExecutionEnvironment. . . . .	239
SetSequenceState. . . . .	241
StartApplication. . . . .	244
StopApplication. . . . .	246

stopBlazeService. . . . .	248
Tag. . . . .	251
untag. . . . .	254
replaceAllTag. . . . .	256
UndeployApplication. . . . .	259
UpdateApplication. . . . .	261
UpdateApplicationOptions. . . . .	263
UpdateComputeOptions. . . . .	264
UpdateDataObjectOptions. . . . .	266
Datenobjektoptionen. . . . .	268
UpdateParameterSetEntries. . . . .	269
UpdateServiceOptions . . . . .	271
Optionen des Datenintegrationsdiensts. . . . .	273
UpdateServiceProcessOptions . . . . .	285
Prozessoptionen des Datenintegrationsdiensts. . . . .	287
Regeln und Richtlinien. . . . .	289
<b>Kapitel 14: infacmd dis-Abfragen. . . . .</b>	<b>290</b>
Abfragen. . . . .	290
Vergleichsoperatoren. . . . .	291
Angabe eines Ordnerpfads. . . . .	292
Logische Operatoren. . . . .	293
Abfrageparameter. . . . .	293
Abfragestruktur. . . . .	295
Where-Klausel. . . . .	295
<b>Kapitel 15: infacmd dp-Befehlsreferenz. . . . .</b>	<b>297</b>
startSparkJobServer. . . . .	297
stopSparkJobServer. . . . .	299
<b>Kapitel 16: infacmd idp-Befehlsreferenz. . . . .</b>	<b>302</b>
createRepository. . . . .	302
createService. . . . .	304
updateService. . . . .	309
upgradeRepository. . . . .	312
<b>Kapitel 17: infacmd edpl-Befehlsreferenz. . . . .</b>	<b>315</b>
createService. . . . .	315
purgeauditevents. . . . .	320
updateService. . . . .	322
upgradeService. . . . .	326

<b>Kapitel 18: Infacmd es-Befehlsreferenz.....</b>	<b>329</b>
ListServiceOptions. . . . .	329
UpdateServiceOptions. . . . .	330
UpdateSMTPOptions. . . . .	331
 <b>Kapitel 19: infacmd ihs-Befehlsreferenz.....</b>	 <b>334</b>
cleanCluster. . . . .	334
createservice. . . . .	336
ListServiceOptions. . . . .	348
ListServiceProcessOptions. . . . .	349
shutdownCluster. . . . .	351
UpdateServiceOptions. . . . .	353
UpdateServiceProcessOptions. . . . .	354
 <b>Kapitel 20: infacmd ipc-Befehlsreferenz.....</b>	 <b>357</b>
ExportToPC. . . . .	357
ImportFromPC. . . . .	361
genReuseReportFromPC. . . . .	363
 <b>Kapitel 21: Infacmd isp-Befehlsreferenz.....</b>	 <b>367</b>
AddAlertUser. . . . .	367
AddConnectionPermissions. . . . .	369
addCustomLDAPType. . . . .	371
AddDomainLink. . . . .	374
AddDomainNode. . . . .	376
AddGroupPrivilege. . . . .	378
addLDAPConnectivity . . . . .	380
AddLicense. . . . .	383
AddNamespace. . . . .	385
AddNodeResource. . . . .	388
AddRolePrivilege. . . . .	390
AddServiceLevel. . . . .	392
AddUserPrivilege. . . . .	394
AddUserToGroup . . . . .	396
AssignDefaultOSProfile. . . . .	398
AssignedToLicense. . . . .	400
AssignGroupPermission . . . . .	402
AssignISToMMSservice. . . . .	404
AssignLicense. . . . .	406
AssignRoleToGroup. . . . .	408
AssignRoleToUser . . . . .	410
AssignRSToWSHubService. . . . .	412

AssignUserPermission . . . . .	414
ConvertLogFile. . . . .	417
convertUserActivityLogFile. . . . .	417
CreateConnection. . . . .	418
Adabas-Verbindungsoptionen. . . . .	424
Amazon Kinesis-Verbindungsoptionen . . . . .	426
Verbindungsoptionen für Amazon Redshift. . . . .	427
Verbindungsoptionen für Amazon S3. . . . .	429
Blockchain-Verbindungsoptionen. . . . .	432
Cassandra-Verbindungsoptionen. . . . .	434
Confluent Kafka-Verbindungsoptionen. . . . .	435
Databricks-Verbindungsoptionen. . . . .	435
DataSift-Verbindungsoptionen. . . . .	436
DB2 für i5/OS-Verbindungsoptionen. . . . .	437
DB2 for z/OS-Verbindungsoptionen. . . . .	439
Facebook-Verbindungsoptionen. . . . .	441
Greenplum-Verbindungsoptionen. . . . .	442
Google Analytics-Verbindungsoptionen. . . . .	443
Google BigQuery-Verbindungsoptionen. . . . .	443
Google Cloud Spanner-Verbindungsoptionen. . . . .	444
Google Cloud Storage-Verbindungsoptionen. . . . .	445
Hadoop Connection Options. . . . .	446
HBase-Verbindungsoptionen. . . . .	451
HDFS-Verbindungsoptionen. . . . .	451
Hive-Verbindungsoptionen. . . . .	452
IBM DB2-Verbindungsoptionen. . . . .	456
IMS-Verbindungsoptionen. . . . .	459
JDBC-Verbindungsoptionen. . . . .	461
JDBC V2-Verbindungsoptionen. . . . .	463
JD Edwards EnterpriseOne-Verbindungsoptionen. . . . .	465
Kafka-Verbindungsoptionen. . . . .	466
Kudu-Verbindungsoptionen. . . . .	467
LDAP-Verbindungsoptionen. . . . .	468
LinkedIn-Verbindungsoptionen. . . . .	468
MapR-DB Connection Options. . . . .	469
Microsoft Azure Blob Storage-Verbindungsoptionen. . . . .	469
Microsoft Azure Data Lake Storage Gen1-Verbindungsoptionen. . . . .	470
Microsoft Azure Data Lake Storage Gen2-Verbindungsoptionen. . . . .	471
Microsoft Azure SQL Data Warehouse-Verbindungsoptionen. . . . .	471
Microsoft SQL Server-Verbindungsoptionen. . . . .	472
Microsoft Dynamics CRM-Verbindungsoptionen. . . . .	475
Netezza-Verbindungsoptionen. . . . .	477

OData-Verbindungsoptionen. . . . .	478
ODBC-Verbindungsoptionen. . . . .	478
Oracle-Verbindungsoptionen. . . . .	480
Salesforce-Verbindungsoptionen. . . . .	483
Salesforce Marketing Cloud-Verbindungsoptionen. . . . .	484
SAPAPPLICATIONS-Verbindungsoptionen. . . . .	485
Sequentielle Verbindungs-Optionen. . . . .	486
Snowflake-Verbindungsoptionen. . . . .	488
Tableau-Verbindungsoptionen. . . . .	489
Tableau V3-Verbindungsoptionen. . . . .	489
Verbindungsoptionen des parallelen Teradata-Transporters. . . . .	490
Twitter-Verbindungsoptionen. . . . .	493
Twitter Streaming-Verbindungsoptionen. . . . .	493
VSAM-Verbindungsoptionen. . . . .	494
Verbindungsoptionen von Web Content-Kapow Katalyst. . . . .	495
CreateFolder. . . . .	496
CreateGrid. . . . .	498
CreateGroup. . . . .	500
CreateIntegrationService. . . . .	502
Integrationsdienst-Optionen. . . . .	506
Integration Service-Prozessoptionen. . . . .	511
CreateMMService. . . . .	513
Metadata Manager-Dienst-Optionen . . . . .	515
CreateOSProfile . . . . .	517
Datenintegrationsdienst-Prozessoptionen für Betriebssystemprofile. . . . .	520
PowerCenter-Integrationsdienst-Prozessoptionen für Betriebssystemprofile. . . . .	521
CreateRepositoryService. . . . .	522
CreateRole. . . . .	527
CreateSAPBWService. . . . .	529
SAP BW Service-Optionen. . . . .	532
SAP BW Service-Prozessoption. . . . .	532
CreateUser . . . . .	533
CreateWSHubService. . . . .	536
Web Services Hub-Optionen. . . . .	538
DeleteNamespace. . . . .	540
DisableNodeResource. . . . .	542
DisableService. . . . .	544
DisableServiceProcess. . . . .	546
DisableUser. . . . .	548
EditUser. . . . .	550
EnableNodeResource. . . . .	553
EnableService. . . . .	555

EnableServiceProcess. . . . .	556
EnableUser . . . . .	558
ExportDomainObjects. . . . .	560
ExportUsersAndGroups. . . . .	563
GetFolderInfo. . . . .	566
GetLastError. . . . .	567
GetLog. . . . .	570
GetNodeName. . . . .	573
GetPasswordComplexityConfig. . . . .	574
getDomainSamlConfig. . . . .	575
GetServiceOption. . . . .	577
GetServiceProcessOption. . . . .	578
GetServiceProcessStatus. . . . .	580
GetServiceStatus. . . . .	582
GetSessionLog. . . . .	584
GetSystemLogDirectory. . . . .	587
getUserActivityLog. . . . .	588
GetWorkflowLog. . . . .	591
Hilfe. . . . .	595
ImportDomainObjects. . . . .	595
ImportUsersAndGroups. . . . .	600
ListAlertUsers. . . . .	602
listAllCustomLDAPTypes. . . . .	604
ListAllGroups. . . . .	605
listAllLDAPConnectivity. . . . .	607
ListAllRoles . . . . .	608
ListAllUsers . . . . .	610
ListConnectionOptions. . . . .	611
ListConnectionPermissions. . . . .	613
ListConnectionPermissionsByGroup. . . . .	615
ListConnectionPermissionsByUser. . . . .	617
ListConnections. . . . .	619
ListConnectionOptions. . . . .	621
listCustomLDAPType. . . . .	622
ListDefaultOSProfiles. . . . .	624
ListDomainCiphers. . . . .	625
ListDomainLinks. . . . .	628
ListDomainOptions. . . . .	630
ListFolders. . . . .	631
ListGridNodes. . . . .	633
ListGroupPermissions. . . . .	634
ListGroupPrivileges. . . . .	636



ListGroupsForUser. . . . .	638
ListLDAPConnectivity . . . . .	640
ListLicenses. . . . .	642
ListMonitoringOptions. . . . .	644
ListNodeOptions. . . . .	645
ListNodeResources. . . . .	647
ListNodeRoles. . . . .	648
ListNodes. . . . .	650
ListOSProfiles. . . . .	652
ListRepositoryLDAPConfiguration. . . . .	654
ListRolePrivileges. . . . .	655
ListSecurityDomains. . . . .	657
ListServiceLevels. . . . .	659
ListServiceNodes. . . . .	660
ListServicePrivileges . . . . .	662
ListServices. . . . .	664
ListSMTPOptions. . . . .	666
ListUserPermissions. . . . .	668
ListUserPrivileges . . . . .	670
infacmd ListWeakPasswordUsers. . . . .	672
migrateUsers. . . . .	674
MoveFolder. . . . .	675
MoveObject. . . . .	677
Ping. . . . .	679
PingDomain. . . . .	680
PrintSPNAndKeytabNames. . . . .	682
PurgeLog. . . . .	683
PurgeMonitoringData. . . . .	685
RemoveAlertUser. . . . .	687
RemoveConnection. . . . .	689
RemoveConnectionPermissions. . . . .	691
removeCustomLDAPType. . . . .	693
RemoveDomainLink. . . . .	695
RemoveFolder. . . . .	697
RemoveGrid. . . . .	699
RemoveGroup. . . . .	700
RemoveGroupPermission . . . . .	702
RemoveGroupPrivilege. . . . .	704
removeLDAPConnectivity. . . . .	706
RemoveLicense. . . . .	708
RemoveNode. . . . .	710
RemoveNodeResource. . . . .	711

RemoveOSProfile. . . . .	713
RemoveRole . . . . .	715
RemoveRolePrivilege . . . . .	717
RemoveService. . . . .	719
RemoveServiceLevel. . . . .	721
RemoveUser. . . . .	723
RemoveUserFromGroup . . . . .	725
RemoveUserPermission . . . . .	726
RemoveUserPrivilege . . . . .	729
RenameConnection. . . . .	731
ResetPassword. . . . .	733
RunCPUProfile. . . . .	735
SetConnectionPermissions. . . . .	737
SetRepositoryLDAPConfiguration . . . . .	739
ShowLicense. . . . .	742
ShutdownNode. . . . .	744
SwitchToGatewayNode. . . . .	745
SwitchToWorkerNode. . . . .	747
SyncSecurityDomains. . . . .	749
UnassignDefaultOSProfile. . . . .	751
UnassignISMMSERVICE. . . . .	752
UnassignLicense. . . . .	754
UnassignRoleFromGroup . . . . .	756
UnassignRoleFromUser. . . . .	758
UnassignRSWSHubService. . . . .	760
UnassociateDomainNode. . . . .	762
UpdateConnection. . . . .	764
updateCustomLDAPType. . . . .	768
UpdateDomainOptions. . . . .	771
UpdateFolder. . . . .	773
UpdateGatewayInfo . . . . .	775
UpdateGrid. . . . .	776
UpdateIntegrationService. . . . .	778
updateLDAPConnectivity. . . . .	781
UpdateLicense. . . . .	784
UpdateMMSERVICE. . . . .	786
UpdateMonitoringOptions. . . . .	788
UpdateNamespace. . . . .	791
UpdateNodeOptions. . . . .	794
UpdateNodeRole. . . . .	796
UpdateOSProfile. . . . .	799
UpdateRepositoryService. . . . .	802

UpdateSAPBWService. . . . .	807
UpdateServiceLevel. . . . .	809
UpdateServiceProcess. . . . .	810
UpdateSMTPOptions. . . . .	813
UpdateWSHubService. . . . .	815
UpgradeGatewayNodeMetadata. . . . .	817
validateFeature. . . . .	819
Version. . . . .	820

## **Kapitel 22: infacmd Idm-Befehlsreferenz..... 821**

backupContents. . . . .	821
CreateService. . . . .	824
ListServiceOptions. . . . .	830
ListServiceProcessOptions. . . . .	832
migrateContents. . . . .	833
publishArchive. . . . .	837
restoreContents. . . . .	839
UpdateServiceOptions. . . . .	842
UpdateServiceProcessOptions. . . . .	844
upgrade. . . . .	846

## **Kapitel 23: infacmd mas-Befehlsreferenz..... 849**

CreateService. . . . .	849
ListServiceOptions. . . . .	853
ListServiceProcessOptions. . . . .	855
UpdateServiceOptions. . . . .	857
Metadaten-Zugriffsdienst-Optionen. . . . .	859
UpdateServiceProcessOptions. . . . .	860
Optionen für Metadaten-Zugriffsdienst-Prozesse. . . . .	862

## **Kapitel 24: infacmd mi-Befehlsreferenz..... 864**

abortRun. . . . .	864
clearSamlConfig. . . . .	865
createService. . . . .	866
deploySpec. . . . .	870
exportSpec. . . . .	871
extendedRunStats. . . . .	872
getSpecRunStats. . . . .	874
listSpecRuns. . . . .	875
listSpecs. . . . .	876
restartMapping. . . . .	877
runSpec. . . . .	879
updateSamlConfig. . . . .	880

<b>Kapitel 25: infacmd mrs-Befehlsreferenz.....</b>	<b>883</b>
BackupContents. . . . .	884
CheckInObject. . . . .	886
CreateContents. . . . .	888
CreateFolder. . . . .	890
CreateProject. . . . .	892
CreateService. . . . .	894
DeleteContents. . . . .	899
DeleteFolder. . . . .	901
DeleteProject. . . . .	903
disableMappingValidationEnvironment. . . . .	905
enableMappingValidationEnvironment. . . . .	909
ListBackupFiles. . . . .	913
ListCheckedOutObjects. . . . .	915
listFolders. . . . .	917
ListLockedObjects . . . . .	919
listMappingEngines. . . . .	921
listPermissionOnProject. . . . .	923
ListProjects. . . . .	925
ListServiceOptions. . . . .	927
ListServiceProcessOptions. . . . .	929
ManageGroupPermissionOnProject. . . . .	931
ManageUserPermissionOnProject. . . . .	933
PopulateVCS. . . . .	935
ReassignCheckedOutObject. . . . .	936
rebuildDependencyGraph. . . . .	938
RenameFolder. . . . .	940
replaceMappingHadoopRuntimeConnections. . . . .	942
RestoreContents. . . . .	944
UndoCheckout. . . . .	946
setMappingExecutionEnvironment. . . . .	948
UndoCheckout. . . . .	950
UnlockObject . . . . .	952
UpdateServiceOptions. . . . .	954
Optionen des Modellrepository-Diensts. . . . .	956
UpdateServiceProcessOptions. . . . .	961
UpdateStatistics. . . . .	963
UpgradeContents. . . . .	965
UpgradeExportedObjects. . . . .	967
 <b>Kapitel 26: infacmd ms-Befehlsreferenz .....</b>	 <b>970</b>
abortAllJobs. . . . .	970

deleteMappingPersistedOutputs. . . . .	972
fetchAggregatedClusterLogs. . . . .	975
getMappingStatus. . . . .	977
getRequestLog. . . . .	979
ListMappingOptions. . . . .	981
listMappingParams. . . . .	982
listMappingParams-Ausgabe. . . . .	984
listMappingPersistedOutputs. . . . .	985
listMappings. . . . .	987
purgeDatabaseWorkTables. . . . .	989
runMapping. . . . .	991
UpdateMappingOptions. . . . .	996
UpdateOptimizationDefaultLevel. . . . .	998
UpdateOptimizationLevel. . . . .	1000
UpgradeMappingParameterFile. . . . .	1002

## **Kapitel 27: Infacmd oie-Befehlsreferenz..... 1005**

## **Kapitel 28: infacmd ps-Befehlsreferenz..... 1006**

cancelProfileExecution. . . . .	1006
CreateWH. . . . .	1008
detectOrphanResults. . . . .	1010
DropWH. . . . .	1011
Execute. . . . .	1013
executeProfile. . . . .	1015
getExecutionStatus. . . . .	1017
getProfileExecutionStatus. . . . .	1019
List. . . . .	1021
ListAllProfiles. . . . .	1023
migrateProfileResults. . . . .	1024
migrateScorecards. . . . .	1026
Purge. . . . .	1028
purgeOrphanResults. . . . .	1030
restoreProfilesAndScorecards. . . . .	1032
synchronizeProfile. . . . .	1034

## **Kapitel 29: infacmd pwx-Befehlsreferenz..... 1037**

CloseForceListener. . . . .	1037
CloseListener. . . . .	1040
CondenseLogger. . . . .	1043
createdatamaps. . . . .	1046
CreateListenerService. . . . .	1049
CreateLoggerService. . . . .	1051

DisplayAllLogger. . . . .	1056
DisplayCPULogger. . . . .	1059
DisplayEventsLogger. . . . .	1062
DisplayMemoryLogger. . . . .	1065
DisplayRecordsLogger. . . . .	1068
displayStatsListener. . . . .	1071
DisplayStatusLogger. . . . .	1074
FileSwitchLogger. . . . .	1077
ListTaskListener. . . . .	1080
ShutDownLogger. . . . .	1083
StopTaskListener. . . . .	1086
UpgradeModels. . . . .	1089
UpdateListenerService. . . . .	1092
UpdateLoggerService. . . . .	1096

## **Kapitel 30: infacmd roh-Befehlsreferenz. . . . . 1101**

listProcessProperties. . . . .	1101
listReverseProxyServerOptions. . . . .	1103
listServiceProcessOptions. . . . .	1104
listServiceOptions. . . . .	1106
updateReverseProxyServerOptions. . . . .	1107
updateServiceProcessOptions. . . . .	1110
updateServiceOptions. . . . .	1111

## **Kapitel 31: infacmd rms-Befehlsreferenz. . . . . 1114**

ListComputeNodeAttributes. . . . .	1114
ListServiceOptions. . . . .	1116
SetComputeNodeAttributes. . . . .	1117
UpdateServiceOptions. . . . .	1119
Optionen des Ressourcenmanager-Diensts. . . . .	1121

## **Kapitel 32: infacmd rtm-Befehlsreferenz. . . . . 1122**

DeployImport. . . . .	1122
Export. . . . .	1124
Import. . . . .	1127

## **Kapitel 33: infacmd sch-Befehlsreferenz. . . . . 1130**

CreateSchedule. . . . .	1130
Gültige Zeitzoneparameter. . . . .	1133
DeleteSchedule. . . . .	1137
ListSchedule. . . . .	1138
listScheduleOfUser. . . . .	1140
ListServiceOptions. . . . .	1140

ListServiceProcessOptions. . . . .	1141
PauseAll. . . . .	1142
PauseSchedule. . . . .	1143
ResumeAll. . . . .	1144
ResumeSchedule. . . . .	1145
UpdateSchedule. . . . .	1146
UpdateServiceOptions. . . . .	1149
Optionen des Scheduler-Diensts. . . . .	1151
UpdateServiceProcessOptions. . . . .	1152
Optionen des Scheduler-Dienstprozesses. . . . .	1153
updateUserPasswordInSchedule. . . . .	1155
Upgrade. . . . .	1156
 <b>Kapitel 34: infacmd search-Befehlsreferenz. . . . .</b>	 <b>1157</b>
CreateService. . . . .	1157
ListServiceOptions. . . . .	1160
ListServiceProcessOptions. . . . .	1162
UpdateServiceOptions. . . . .	1164
UpdateServiceProcessOptions. . . . .	1166
 <b>Kapitel 35: infacmd sql-Befehlsreferenz. . . . .</b>	 <b>1168</b>
ExecuteSQL. . . . .	1168
ListColumnOptions. . . . .	1169
ListColumnPermissions. . . . .	1171
ListSQLDataServiceOptions. . . . .	1173
ListSQLDataServicePermissions. . . . .	1175
ListSQLDataServices. . . . .	1176
ListStoredProcedurePermissions. . . . .	1178
ListTableOptions. . . . .	1180
ListTablePermissions. . . . .	1182
PurgeTableCache. . . . .	1183
RefreshTableCache . . . . .	1185
RenameSQLDataService. . . . .	1187
SetColumnPermissions. . . . .	1189
SetSQLDataServicePermissions. . . . .	1191
SetStoredProcedurePermissions. . . . .	1194
SetTablePermissions. . . . .	1197
StartSQLDataService. . . . .	1199
StopSQLDataService. . . . .	1201
UpdateColumnOptions. . . . .	1203
Spaltenoptionen. . . . .	1205
UpdateSQLDataServiceOptions. . . . .	1206
SQL-Datendienst-Optionen. . . . .	1207

UpdateTableOptions. . . . .	1209
Virtuelle Tabellenoptionen. . . . .	1211
<b>Kapitel 36: infacmd tdm-Befehlsreferenz. . . . .</b>	<b>1212</b>
CreateService. . . . .	1212
CreateContents. . . . .	1218
EnableService. . . . .	1220
DisableService. . . . .	1221
<b>Kapitel 37: infacmd tools-Befehlsreferenz. . . . .</b>	<b>1224</b>
deployApplication. . . . .	1224
exportObjects. . . . .	1226
exportResources. . . . .	1228
importObjects. . . . .	1230
patchApplication. . . . .	1234
<b>Kapitel 38: infacmd wfs-Befehlsreferenz. . . . .</b>	<b>1237</b>
abortWorkflow. . . . .	1237
bulkComplete. . . . .	1239
cancelWorkflow. . . . .	1241
completeTask. . . . .	1243
createTables. . . . .	1245
delegateTask. . . . .	1247
dropTables. . . . .	1249
listActiveWorkflowInstances. . . . .	1251
listMappingPersistedOutputs. . . . .	1253
listTasks. . . . .	1255
listWorkflowParams. . . . .	1258
listWorkflowParams-Ausgabe. . . . .	1260
listWorkflows. . . . .	1261
pruneOldInstances. . . . .	1263
recoverWorkflow. . . . .	1265
releaseTask. . . . .	1267
setMappingPersistedOutputs. . . . .	1269
startTask. . . . .	1272
startWorkflow. . . . .	1273
upgradeWorkflowParameterFile. . . . .	1276
<b>Kapitel 39: infacmd ws-Befehlsreferenz. . . . .</b>	<b>1279</b>
ListOperationOptions. . . . .	1279
ListOperationPermissions. . . . .	1281
ListWebServiceOptions. . . . .	1283
ListWebServicePermissions. . . . .	1285



ListWebServices. . . . .	1287
RenameWebService. . . . .	1289
SetOperationPermissions. . . . .	1291
SetWebServicePermissions. . . . .	1294
StartWebService. . . . .	1297
StopWebService. . . . .	1299
UpdateOperationOptions. . . . .	1300
Operationsoptionen. . . . .	1302
UpdateWebServiceOptions. . . . .	1303
Web-Dienst-Optionen. . . . .	1305
<b>Kapitel 40: infacmd xrf-Befehlsreferenz. . . . .</b>	<b>1307</b>
generateReadableViewXML. . . . .	1307
updateExportXML. . . . .	1308
<b>Kapitel 41: infacmd-Steuerdateien. . . . .</b>	<b>1309</b>
infacmd-Steuerdateien - Übersicht. . . . .	1309
Konfiguration von Steuerdateien. . . . .	1309
Benennungskonventionen für Steuerdateien. . . . .	1310
Exportsteuerdateien. . . . .	1310
Export-Steuerdatei-Parameter für Domänenobjekte. . . . .	1311
Exportsteuerdateiparameter für Modellrepository-Objekte. . . . .	1312
Importsteuerdateien. . . . .	1315
Import-Steuerdatei-Parameter für Domänenobjekte. . . . .	1316
Importsteuerdateiparameter für Modellrepository-Objekte. . . . .	1318
Regeln und Richtlinien für Steuerdateien. . . . .	1323
Steuerdatei-Beispiele für Domänenobjekte. . . . .	1324
Steuerdatei-Beispiele für Model Repository-Objekte. . . . .	1325
<b>Kapitel 42: infasetup-Befehlsreferenz. . . . .</b>	<b>1327</b>
Verwenden von infasetup. . . . .	1328
Ausführen von Befehlen. . . . .	1328
Befehlsoptionen. . . . .	1328
infasetup Befehlsreferenz. . . . .	1328
Verwenden von Datenbankverbindungsstrings. . . . .	1329
BackupDomain. . . . .	1329
DefineDomain. . . . .	1332
DefineGatewayNode. . . . .	1342
DefineWorkerNode. . . . .	1348
DeleteDomain. . . . .	1353
GenerateEncryptionKey. . . . .	1356
Hilfe. . . . .	1356
ListDomainCiphers. . . . .	1357

MigrateEncryptionKey. . . . .	1358
RestoreDomain. . . . .	1359
restoreMitKerberosLinkage. . . . .	1362
SwitchToKerberosMode. . . . .	1363
UpdateDomainCiphers. . . . .	1364
updateDomainName. . . . .	1367
UpdateGatewayNode. . . . .	1367
UpdateKerberosAdminUser. . . . .	1373
UpdateKerberosConfig. . . . .	1373
updateMitKerberosLinkage. . . . .	1374
UpdatePasswordComplexityConfig. . . . .	1376
updateDomainSamlConfig. . . . .	1376
UpdateWorkerNode. . . . .	1379
upgradeDomainMetadata. . . . .	1384
UpgradeGatewayNodeMetadata. . . . .	1386
UnlockUser. . . . .	1388
ValidateandRegisterFeature. . . . .	1389

## **Kapitel 43: Pmcmd-Befehlsreferenz. . . . . 1391**

Verwenden von pmcmd. . . . .	1392
Ausführen von Befehlen im Befehlszeilenmodus. . . . .	1392
Ausführen von Befehlen im interaktiven Modus. . . . .	1394
Ausführen im wait-Modus. . . . .	1395
Scripting von pmcmd-Befehlen. . . . .	1396
Eingeben von Befehlsoptionen. . . . .	1396
aborttask. . . . .	1397
abortworkflow. . . . .	1399
Connect. . . . .	1401
Disconnect. . . . .	1402
Exit. . . . .	1403
getrunningsessionsdetails. . . . .	1403
GetServiceDetails. . . . .	1404
getserviceproperties. . . . .	1406
getsessionstatistics. . . . .	1407
gettaskdetails. . . . .	1409
getworkflowdetails. . . . .	1411
help. . . . .	1415
pingservice. . . . .	1415
recoverworkflow. . . . .	1416
scheduleworkflow. . . . .	1418
SetFolder. . . . .	1420
SetNoWait. . . . .	1420
SetWait. . . . .	1421

ShowSettings. . . . .	1421
StartTask. . . . .	1421
Verwenden von Parameterdateien mit starttask. . . . .	1424
StartWorkflow. . . . .	1425
Verwenden von Parameterdateien mit startworkflow. . . . .	1428
StopTask. . . . .	1429
StopWorkflow. . . . .	1431
UnscheduleWorkflow. . . . .	1433
UnsetFolder. . . . .	1435
Version. . . . .	1435
WaitTask. . . . .	1435
WaitWorkflow. . . . .	1437

## **Kapitel 44: pmrep-Befehlsreferenz..... 1440**

Verwenden von pmrep. . . . .	1442
Ausführen von Befehlen im Befehlszeilenmodus. . . . .	1442
Ausführen von Befehlen im interaktiven Modus. . . . .	1442
Ausführen von Befehlen im normalen und exklusiven Modus. . . . .	1443
pmrep-Rückgabewerte. . . . .	1443
Verwenden von nativen Verbindungsstrings. . . . .	1443
pmrep-Scripting-Befehle. . . . .	1444
Verbindungsuntertypen. . . . .	1445
AddToDeploymentGroup. . . . .	1447
ApplyLabel. . . . .	1449
AssignIntegrationService. . . . .	1451
AssignPermission. . . . .	1452
Beispiel. . . . .	1453
BackUp. . . . .	1454
ChangeOwner. . . . .	1455
CheckIn. . . . .	1455
CleanUp. . . . .	1456
ClearDeploymentGroup. . . . .	1456
Connect. . . . .	1457
Create. . . . .	1459
CreateConnection. . . . .	1460
Festlegen der Datenbank-Codepage. . . . .	1463
CreateDeploymentGroup. . . . .	1464
CreateFolder. . . . .	1464
Zuweisen von Berechtigungen. . . . .	1465
CreateLabel. . . . .	1466
CreateQuery. . . . .	1466
Delete. . . . .	1472
DeleteConnection. . . . .	1473

DeleteDeploymentGroup. . . . .	1474
DeleteFolder. . . . .	1474
DeleteLabel. . . . .	1475
DeleteObject. . . . .	1475
DeleteQuery. . . . .	1476
DeployDeploymentGroup. . . . .	1477
DeployFolder. . . . .	1478
ExecuteQuery. . . . .	1480
Exit. . . . .	1482
FindCheckout. . . . .	1482
GetConnectionDetails. . . . .	1484
GenerateAbapProgramToFile. . . . .	1484
Hilfe. . . . .	1486
InstallAbapProgram. . . . .	1486
KillUserConnection. . . . .	1489
ListConnections. . . . .	1489
ListObjectDependencies. . . . .	1490
ListObjects. . . . .	1492
Listing Object Types. . . . .	1494
Auflisten von Ordnern. . . . .	1497
Auflisten von Objekten. . . . .	1497
ListTablesBySess. . . . .	1498
ListUserConnections. . . . .	1499
MassUpdate. . . . .	1499
Sitzungseigenschafts-Typen. . . . .	1501
Regeln und Richtlinien für MassUpdate. . . . .	1505
Beispiel-Protokolldatei. . . . .	1505
ModifyFolder. . . . .	1505
Benachrichtigen. . . . .	1507
ObjectExport. . . . .	1507
Beispiele. . . . .	1509
ObjectImport. . . . .	1509
PurgeVersion. . . . .	1510
Beispiele. . . . .	1513
Register. . . . .	1513
RegisterPlugin. . . . .	1515
Registrieren eines Sicherheitsmoduls. . . . .	1516
Beispiel. . . . .	1516
Wiederherstellen. . . . .	1517
Beispiel. . . . .	1518
RollbackDeployment. . . . .	1518
Beispiel. . . . .	1519

Ausführen. . . . .	1519
ShowConnectionInfo. . . . .	1520
SwitchConnection. . . . .	1520
TruncateLog. . . . .	1521
UndoCheckout. . . . .	1522
Unregister. . . . .	1523
UnregisterPlugin. . . . .	1524
Aufheben der Registrierung eines externen Sicherheitsmoduls. . . . .	1525
Beispiel. . . . .	1526
UpdateConnection. . . . .	1526
UpdateEmailAddr. . . . .	1528
UpdateSeqGenVals. . . . .	1529
UpdateSrcPrefix. . . . .	1530
UpdateStatistics . . . . .	1531
UpdateTargPrefix. . . . .	1532
Upgrade. . . . .	1533
UninstallAbapProgram. . . . .	1533
Validieren. . . . .	1535
Version. . . . .	1537

## **Kapitel 45: Arbeiten mit filemanager..... 1538**

filemanager Overview. . . . .	1538
Default Behavior. . . . .	1539
Guidelines. . . . .	1539
copy. . . . .	1540
copyfromlocal. . . . .	1541
list. . . . .	1542
move. . . . .	1543
remove. . . . .	1545
rename. . . . .	1546
watch. . . . .	1547

## **Kapitel 46: Arbeiten mit pmrep-Dateien..... 1550**

Arbeiten mit pmrep-Dateien - Übersicht. . . . .	1550
Verwenden der persistenten Eingabedatei . . . . .	1550
Erstellen einer persistenten Eingabedatei mit pmrep. . . . .	1551
Manuelles Erstellen einer persistenten Eingabedatei. . . . .	1552
Verwenden der Objektimport-Steuerdatei. . . . .	1553
Objektimport-Steuerdatei-Parameter. . . . .	1554
Objektimport-Steuerdatei – Beispiele. . . . .	1557
Importieren von Quellobjekten. . . . .	1558
Importieren von mehreren Objekten in einen Ordner. . . . .	1559
Einchecken der und Beschriften von importierten Objekten. . . . .	1559

Beibehalten von Sequenzgenerator- und Normalisierungsprogramm-Werten. . . . .	1559
Importieren von Objekten und lokalen Shortcut-Objekten zum selben Repository. . . . .	1560
Importieren von Shortcut-Objekten aus einem anderen Repository. . . . .	1560
Importieren von Objekten in mehrere Ordner. . . . .	1560
Importieren von spezifischen Objekten. . . . .	1561
Wiederverwenden und Ersetzen von abhängigen Objekten. . . . .	1561
Ersetzen ungültiger Mappings. . . . .	1562
Umbenennen von Objekten. . . . .	1562
Kopieren von SAP-Mappings und SAP-Programminformationen. . . . .	1563
Anwenden von Standard-Verbindungsattributen. . . . .	1563
Auflösen von Objektkonflikten. . . . .	1563
Verwenden der Bereitstellungssteuerdatei . . . . .	1564
Bereitstellungs-Steuerdatei-Parameter. . . . .	1566
Bereitstellungs-Steuerdatei – Beispiele. . . . .	1571
Bereitstellen der aktuellen Version eines Ordners. . . . .	1571
Bereitstellen der aktuellen Version einer Bereitstellungsgruppe. . . . .	1571
Auflisten mehrerer Quell- und Target-Ordner . . . . .	1572
Tipps für die Arbeit mit pmrep-Dateien. . . . .	1572
<b>Index. . . . .</b>	<b>1574</b>

# Einleitung

Informationen zu den Befehlszeilen- und -Dienstprogrammen, wie z. B. `infacmd`, `infasetup`, `pmcmd`, `pmpasswd` und `pmrep`, zum Verwalten der Informatica-Domäne, der Anwendungsdienste und Objekte finden Sie in der *Informatica®-Befehlsreferenz*. Hier erfahren Sie mehr über Befehlsbeschreibungen, -optionen und -argumente. Sie können einen Großteil der Befehlszeilenfunktionen über das Administrator Tool und andere Client-Tools durchführen.

## Informatica-Ressourcen

Informatica stellt Ihnen über das Informatica-Netzwerk und andere Online-Portale zahlreiche Produktressourcen zur Verfügung. Nutzen Sie die Ressourcen, um Ihre Informatica-Produkte und -Lösungen optimal zu nutzen und von anderen Informatica-Benutzern und Fachspezialisten zu lernen.

### Informatica Network

Das Informatica Network bietet Zugriff auf zahlreiche Ressourcen, darunter die Informatica-Wissensdatenbank und der globale Kundensupport von Informatica. Um auf das Informatica Network zuzugreifen, besuchen Sie <https://network.informatica.com>.

Als Mitglied des Informatica Network haben Sie die folgenden Optionen:

- Durchsuchen Sie die Wissensdatenbank nach Produktressourcen.
- Zeigen Sie Informationen zur Produktverfügbarkeit an.
- Erstellen und überprüfen Sie Ihre Supportfälle.
- Ihr lokales Informatica Network für Benutzergruppen suchen und mit anderen Benutzern zusammenarbeiten.

### Informatica-Wissensdatenbank

In der Informatica-Wissensdatenbank finden Sie Produktressourcen wie beispielsweise praktische Anleitungen, Best Practices, Videotutorials und Antworten auf häufig gestellte Fragen.

Für die Suche in der Wissensdatenbank besuchen Sie <https://search.informatica.com>. Wenn Sie Fragen, Kommentare oder Ideen zur Wissensdatenbank haben, wenden Sie sich per E-Mail an das Team der Informatica-Wissensdatenbank unter [KB\\_Feedback@informatica.com](mailto:KB_Feedback@informatica.com).

## Informatica-Dokumentation

Verwenden Sie das Informatica-Dokumentationsportal, um in einer umfangreichen Dokumentationsbibliothek nach aktuellen und neuen Produktversionen zu suchen. Um das Dokumentationsportal zu erkunden, besuchen Sie <https://docs.informatica.com>

Wenn Sie Fragen, Kommentare oder Ideen zur Produktdokumentation haben, wenden Sie sich an das Informatica-Dokumentationsteam unter [infa\\_documentation@informatica.com](mailto:infa_documentation@informatica.com)

## Informatica-Produktverfügbarkeitsmatrizen

Produktverfügbarkeitsmatrizen (PAMs) geben die Versionen der Betriebssysteme, Datenbanken und Typen von Datenquellen und Zielen an, die in einer Produktversion unterstützt werden. Sie können die Informatica-PAMs unter <https://network.informatica.com/community/informatica-network/product-availability-matrices> durchsuchen.

## Informatica Velocity

Informatica Velocity ist eine Sammlung von Tipps und Best Practices, die von den Professionellen Informatica-Diensten entwickelt wurden und auf praktischen Erfahrungen aus Hunderten von Datenmanagementprojekten basieren. Informatica Velocity umfasst das gesammelte Wissen von Informatica-Beratern, die mit Unternehmen auf der ganzen Welt zusammenarbeiten, um erfolgreiche Datenmanagementlösungen zu planen, zu entwickeln, bereitzustellen und zu warten.

Die Informatica Velocity-Ressourcen finden Sie unter <http://velocity.informatica.com>. Wenn Sie Fragen, Anregungen oder Ideen zu Informatica Velocity haben, wenden Sie sich an die professionellen Informatica-Dienste unter [ips@informatica.com](mailto:ips@informatica.com).

## Informatica Marketplace

Informatica Marketplace ist ein Forum, das Lösungen zur Erweiterung und Verbesserung Ihrer Informatica-Implementierungen bereitstellt. Nutzen Sie die zahlreichen Lösungen von Informatica-Entwicklern und -Partnern im Marketplace, um Ihre Produktivität zu steigern und die Implementierungsdauer Ihrer Projekte zu verkürzen. Den Informatica Marketplace finden Sie unter <https://marketplace.informatica.com>.

## Globaler Kundensupport von Informatica

Sie können sich telefonisch oder über das Informatica-Netzwerk an ein Global Support-Center wenden.

Die Telefonnummer des globalen Kundensupports von Informatica vor Ort finden Sie auf der Informatica-Website unter folgender Verknüpfung:

<https://www.informatica.com/services-and-training/customer-success-services/contact-us.html>.

Um im Informatica-Netzwerk nach Online-Supportressourcen zu suchen, besuchen Sie <https://network.informatica.com> und wählen Sie die eSupport-Option aus.



# KAPITEL 1

## Befehlszeilenprogramme und Dienstprogramme

- [Befehlszeilenprogramme und Dienstprogramme - Übersicht, 29](#)

### Befehlszeilenprogramme und Dienstprogramme - Übersicht

Die Informatica-Installation umfasst Kundensupport-Tools, Befehlszeilenprogramme und Dienstprogramme. Verwenden Sie die Befehlszeilenprogramme und Dienstprogramme zum Verwalten der Informatica-Domäne, der Anwendungsdienste und Objekte. Sie können die Befehlszeilenprogramme und Dienstprogramme auf jedem Rechner ausführen, der auf die Informatica-Domäne zugreifen kann.

Bei Installation der Informatica-Dienste oder -Clients werden die Befehlszeilenprogramme und Dienstprogramme standardmäßig installiert. Durch Installieren der Informatica-Dienstprogramme können Sie die Programme auch auf anderen Rechnern installieren und ausführen.

In der folgenden Tabelle werden die Informatica-Dienstprogramme beschrieben:

Befehlszeilenprogramm	Beschreibung
infacmd	Verwalten der Informatica-Domäne und -Anwendungsdienste und -prozesse, einschließlich der Repository- und Integrationsdienste. Außerdem können Sie mithilfe von infacmd Lizenzen und Protokollereignisse verwalten und darauf zugreifen sowie Objekte und Benutzerkonten exportieren und importieren.
infasetup	Verwalten von Domänen und Knoten.
filemanager	Verwalten Sie die Vorverarbeitungs- und Dateiüberwachungsfunktionen für ein Cloud-Ökosystem.

In der folgenden Tabelle werden die PowerCenter®-Dienstprogramme beschrieben:

Befehlszeilenprogramm	Beschreibung
pmcmd	Verwalten von Arbeitsabläufen. Mithilfe von pmcmd können Sie Arbeitsabläufe starten, anhalten, planen und überwachen.
pmpasswd	Dient zum Verschlüsseln von mit den Umgebungsvariablen pmcmd und pmrep zu verwendenden Passwörtern.
pmrep	Führt Verwaltungsaufgaben für das Repository durch. Mithilfe von pmrep können Sie Repository-Objekte auflisten, Gruppen erstellen und bearbeiten und Repositories wiederherstellen und löschen.

## KAPITEL 2

# Installieren und Konfigurieren von Befehlszeilendienstprogrammen

Dieses Kapitel umfasst die folgenden Themen:

- [Installieren und Konfigurieren von Befehlszeilendienstprogrammen – Übersicht, 31](#)
- [Installieren der Befehlszeilendienstprogramme, 32](#)
- [Konfigurieren der Befehlszeilendienstprogramme, 33](#)
- [Sicherheitskonfiguration für Informatica-Dienstprogramme, 35](#)

## Installieren und Konfigurieren von Befehlszeilendienstprogrammen – Übersicht

Bei der Installation der Informatica-Dienste oder der Informatica-Clients werden die Befehlszeilendienstprogramme standardmäßig installiert. Zudem können Sie die Befehlszeilendienstprogramme auf allen Computern installieren und ausführen, ohne die Informatica-Produkte zu installieren.

Führen Sie folgende Aufgaben aus, um die Befehlszeilendienstprogramme auf einem Computer zu installieren und konfigurieren, auf dem keine Informatica-Produkte installiert sind:

- Installieren Sie die Befehlszeilendienstprogramme.
- Konfigurieren Sie die Befehlszeilendienstprogramme.

Bevor Sie die Befehlszeilendienstprogramme ausführen, müssen Sie die Umgebungsvariablen für die Befehlszeilendienstprogramme konfigurieren. Außerdem müssen Sie Benutzerkonten, die die Befehle ausführen, die Ausführungsberechtigung für die Dienstprogrammdateien gewähren.

- Konfigurieren Sie die Sicherheit für die Befehlszeilendienstprogramme.

Wenn die sichere Kommunikation für die Domäne aktiviert ist oder wenn die Domäne die Kerberos-Authentifizierung verwendet, führen Sie die Sicherheitskonfiguration auf denjenigen Computern aus, auf denen die Befehlszeilendienstprogramme installiert sind.

# Installieren der Befehlszeilendienstprogramme

Informatica stellt eine separate ZIP-Datei für die Installation der Befehlszeilendienstprogramme auf einem Computer bereit, auf dem keine Informatica-Produkte installiert sind.

1. Wenden Sie sich an den globalen Kundensupport von Informatica, um die ZIP-Datei mit den Befehlszeilendienstprogrammen abzurufen.
2. Extrahieren Sie die Dateien auf dem Computer, auf dem die Befehlszeilendienstprogramme ausgeführt werden sollen.
3. Installieren Sie auf Windows das verteilbare Paket von Microsoft Visual Studio 2013, das in den extrahierten Dateien enthalten ist. Führen Sie die 32-Bit- bzw. 64-Bit-Datei aus, die sich im folgenden Verzeichnis befindet:

```
<Utilities installation directory>/PowerCenter/server/VS2013
```

Informatica-Produkte unter Windows benötigen das verteilbare Paket von Microsoft Visual Studio 2013. Beim Installieren der Informatica-Dienste oder der Informatica-Clients installiert das Installationsprogramm das verteilbare Paket für Sie. Wenn Sie die eigenständigen Befehlszeilendienstprogramme installieren, ist das verteilbare Paket in den extrahierten Dateien enthalten, und Sie müssen das Paket manuell installieren.

## Installationsverzeichnisse

Die Installationsverzeichnisse der Befehlszeilendienstprogramme variieren basierend auf den bei der Installation der Informatica-Dienste, der Informatica-Client-Installation oder der Standalone-Installation der Befehlszeilendienstprogramme installierten Dienstprogramme.

### Installation von Informatica-Diensten

Die Informatica-Dienstprogramme sind im folgenden Verzeichnis installiert:

```
<Informatica-Installationsverzeichnis>/isp/bin
```

Die PowerCenter-Dienstprogramme sind im folgenden Verzeichnis installiert:

```
<Informatica-Installationsverzeichnis>/server/bin
```

Die Metadata Manager-Dienstprogramme sind in folgendem Verzeichnis installiert:

```
<Informatica-Installationsverzeichnis>/services/MetadataManagerService/utilities
```

### Installation des Informatica-Clients

Wenn Sie das Developer-Tool installieren, werden die Informatica-Dienstprogramme im folgenden Verzeichnis installiert:

```
<Informatica-Installationsverzeichnis>/clients/DeveloperClient/infacmd
```

Wenn Sie den PowerCenter-Client installieren, werden die PowerCenter-Dienstprogramme im folgenden Verzeichnis installiert:

```
<Informatica-Installationsverzeichnis>/clients/PowerCenterClient/CommandLineUtilities/PC/server/bin
```

Wenn Sie den PowerCenter-Client installieren, werden die Metadata Manager-Dienstprogramme im folgenden Verzeichnis installiert:

```
<Informatica-Installationsverzeichnis>/clients/PowerCenterClient/CommandLineUtilities/MM
```

### Dienstprogramminstallation über die Befehlszeile

Die Informatica-Dienstprogramme sind im folgenden Verzeichnis installiert:

<Dienstprogramm-Installationsverzeichnis>/PowerCenter/isp/bin

Die PowerCenter-Dienstprogramme sind im folgenden Verzeichnis installiert:

<Dienstprogramm-Installationsverzeichnis>/PowerCenter/server/bin

Die Metadata Manager-Dienstprogramme sind in folgendem Verzeichnis installiert:

<Dienstprogramm-Installationsverzeichnis>/MetadataManager/utilities

## Konfigurieren der Befehlszeilendienstprogramme

Konfigurieren Sie den Pfad und die Umgebungsvariablen in Übereinstimmung mit den Befehlszeilendienstprogrammen. Gewähren Sie Benutzerkonten, die die Befehle ausführen, die Ausführungsberechtigung für die Dienstprogrammdateien.

### Konfigurieren der Informatica-Dienstprogramme

Konfigurieren der Umgebungsvariablen für die Befehlszeilenprogramme infacmd und infasetup.

Legen Sie zum Ausführen von infacmd die Umgebungsvariable ICMD\_JAVA\_OPTS fest.

Legen Sie zum Ausführen von infasetup die Umgebungsvariable INFA\_JAVA\_CMD\_OPTS fest.

### Konfigurieren der PowerCenter-Dienstprogramme

Bevor Sie die PowerCenter-Dienstprogramme verwenden, konfigurieren Sie die Programmdateien und Variablen gemäß den folgenden Richtlinien:

- Kopieren Sie zum Ausführen von „pmrep“, „pmcmd“ und „pmpasswd“ die Datei „domains.infa“ für die Informatica-Domäne in das Verzeichnis für Dienstprogramme.
- Zum Ausführen von pmrep, pmcmd und pmpasswd unter UNIX müssen Sie INFA\_HOME, die Umgebungsvariable PATH und die Bibliothekspfad-Umgebungsvariable für den Speicherort der Dienstprogramme festlegen.

Wenn zum Beispiel die Befehlszeilendienstprogramme im Ordner /data/Informatica\_cmd\_utilities/ installiert sind, befinden sich die PowerCenter-Dienstprogramme im Ordner /data/Informatica\_cmd\_utilities/PowerCenter/server/bin. Unter Linux können Sie die Umgebungsvariablen an der Eingabeaufforderung wie folgt festlegen:

```
setenv INFA_HOME /data/Informatica_cmd_utilities/PowerCenter/  
setenv PATH ./data/Informatica_cmd_utilities/PowerCenter/server/bin:$PATH  
setenv LD_LIBRARY_PATH ./data/Informatica_cmd_utilities/PowerCenter/server/  
bin:$LD_LIBRARY_PATH
```

**Hinweis:** Starten Sie den Computer neu, nachdem Sie die INFA\_HOME-Umgebungsvariable oder die Bibliothekspfad-Umgebungsvariable konfiguriert haben.

## Konfigurieren der Metadata Manager-Dienstprogramme

Um Metadata Manager-Dienstprogramme zu konfigurieren, konfigurieren Sie Umgebungsvariablen, die den Speicherort der Java Virtual Machine und das Informatica-Root-Verzeichnis angeben.

Wenn die Domäne die Kerberos-Authentifizierung verwendet, erstellen Sie die Datei „domains.infa“. Metadata Manager-Befehlszeilenprogramme verwenden die Datei „domains.infa“ zum Abrufen von Informationen zur Gateway-Konnektivität für die Domäne.

Konfigurieren Sie die folgenden Umgebungsvariablen:

### JAVA\_HOME

Gibt den Speicherort der Java Virtual Machine an. Legen Sie als JAVA\_HOME das PowerCenter Java-Verzeichnis in der Installation der Befehlszeilendienstprogramme fest. Beispiel:

```
<Dienstprogramm-Installationsverzeichnis>\PowerCenter\java
```

Legen Sie diese Umgebungsvariable in allen Metadata Manager-Befehlszeilenprogrammen wie folgt fest:

1. Öffnen Sie die Batchdatei oder das Shell-Skript mit einem Texteditor.
2. Suchen Sie die Zeile, die als JAVA\_HOME den Wert @INFA\_JDK\_HOME@ festlegt.
3. Ersetzen Sie die Zeichenfolge @INFA\_JDK\_HOME@ mit dem PowerCenter-Java-Verzeichnis. Beispiel:  

```
set JAVA_HOME=C:\InfaUtilities\PowerCenter\java
```
4. Speichern und schließen Sie die Batchdatei bzw. das Shell-Skript.

### INFA\_HOME

Gibt das Informatica-Root-Verzeichnis an, damit alle Informatica-Anwendungen und -Dienste die anderen Informatica-Komponenten, die sie ausführen müssen, finden können. Setzen Sie als INFA\_HOME das PowerCenter-Verzeichnis in der Installation des Befehlszeilen-Dienstprogramms fest. Beispiel:

```
<Dienstprogramm-Installationsverzeichnis>\PowerCenter
```

Legen Sie diese Umgebungsvariable auf jedem Rechner fest, auf dem Sie die Informatica-Dienstprogramme installiert haben.

**Hinweis:** Starten Sie nach dem Konfigurieren von INFA\_HOME den Computer neu.

## Erstellen der Datei „domains.infa“

Die Datei „domains.infa“ enthält die Informationen zur Gateway-Konnektivität für die Domäne. Wenn die Domäne die Kerberos-Authentifizierung verwendet, erstellen Sie die Datei „domains.infa“, damit die Befehlszeilenprogramme die Informationen zur Gateway-Konnektivität für die Domäne abrufen können.

Wenn die Domäne die Kerberos-Authentifizierung verwendet, müssen Sie bei der Ausführung der meisten Befehle von Befehlszeilenprogrammen Informationen zur Domänenkonnektivität eingeben. Geben Sie die Informationen zur Domänenkonnektivität über die Option „--domainName“ oder über die Option „--gateway“ ein. Für die Verwendung der Option „--domainName“ muss die Datei „domains.infa“ die Informationen zur Gateway-Konnektivität für die Domäne enthalten. Wenn die Datei „domains.infa“ nicht vorhanden ist oder die Informationen in der Datei nicht mehr aktuell sind, müssen Sie beim Ausführen von Befehlen, die eine Verbindung zur Domäne herstellen, die Option „--gateway“ verwenden.

Wenn Sie Informatica-Dienste installieren, ist die Datei „domains.infa“ im INFA\_HOME-Verzeichnis verfügbar. Erstellen Sie die Datei für alle anderen Installationen und stellen Sie sicher, dass sie auf dem Computer verfügbar ist, auf dem Sie die Befehle ausführen möchten.

Führen Sie zum Erstellen der Datei „domains.infa“ den Befehl `infacmd isp UpdateGatewayInfo` aus. Der Befehl erstellt oder aktualisiert die Datei „domains.infa“ im PowerCenter-Verzeichnis in der Installation des

Befehlszeilen-Dienstprogramms, beispielsweise <Dienstprogramm-Installationsverzeichnis>  
\PowerCenter.

## Sicherheitskonfiguration für Informatica-Dienstprogramme

Wenn Sie Informatica-Dienstprogramme installieren, müssen Sie die Rechner evtl. auf Basis der Sicherheitskonfiguration für die Domäne konfigurieren. Bei falscher Konfiguration der Rechner können die Befehlszeilenprogramme Benutzer bei der Domäne möglicherweise nicht authentifizieren.

Konfigurieren Sie die Rechner, auf denen Sie die Informatica-Dienstprogramme installiert haben, wenn die Domäne die folgenden Sicherheitskonfigurationen verwendet:

### **Sichere Kommunikation**

Wenn die sichere Kommunikation für die Domäne aktiviert ist, müssen Sie die Rechner möglicherweise für die Verwendung der Truststore-Datei konfigurieren. Wenn Sie eine benutzerdefinierte Truststore-Datei verwenden, müssen Sie Umgebungsvariablen konfigurieren, die das Truststore-Dateiverzeichnis und das Truststore-Passwort angeben.

### **Kerberos-Authentifizierung**

Verwendet die Domäne die Kerberos-Authentifizierung, müssen Sie die Kerberos-Konfigurationsdatei auf die Rechner kopieren, auf denen Sie die Informatica-Dienstprogramme installiert haben. Außerdem müssen Sie die Rechner so konfigurieren, dass sie die Kerberos-Konfigurationsdatei für die Domäne finden.

### **VERWANDTE THEMEN:**

- [“Ausführen von Befehlen in einer sicheren Domäne” auf Seite 39](#)
- [“Ausführen von Befehlen unter UNIX mit Kerberos-Authentifizierung” auf Seite 40](#)
- [“Ausführen von Befehlen unter Windows mit Kerberos-Authentifizierung” auf Seite 41](#)

# KAPITEL 3

## Verwenden der Befehlszeilenprogramme

Dieses Kapitel umfasst die folgenden Themen:

- [Verwenden der Befehlszeilenprogramme - Übersicht, 36](#)
- [Eingeben von Optionen und Argumenten, 37](#)
- [Syntax-Notation, 38](#)
- [Ausführen von Befehlen in einer sicheren Domäne, 39](#)
- [Ausführen von Befehlen unter UNIX mit Kerberos-Authentifizierung, 40](#)
- [Ausführen von Befehlen unter Windows mit Kerberos-Authentifizierung, 41](#)

## Verwenden der Befehlszeilenprogramme - Übersicht

Informatica enthält Befehlszeilenprogramme, mit denen Sie Aufgaben von jedem Rechner in der Informatica-Umgebung aus durchführen können. Die Befehlszeilenprogramme ermöglichen Ihnen, ausgewählte Aufgaben auszuführen, die Sie in Informatica Administrator durchführen können.

Sie können beispielsweise einen Repository-Dienst über das Administrator-Tool oder das `infacmd`-Befehlszeilenprogramm aktivieren oder deaktivieren.

Informatica enthält die folgenden Befehlszeilenprogramme:

- **infacmd.** Verwenden Sie `infacmd` zum Zugreifen auf die Informatica-Anwendungsdienste.
- **infasetup.** Verwenden Sie `infasetup` zum Durchführen von Installationsaufgaben, wie z. B. dem Definieren eines Knotens oder einer Domäne.
- **pmcmd.** Verwenden Sie `pmcmd` zum Verwalten von Arbeitsabläufen. Sie können mit `pmcmd` Arbeitsabläufe starten, stoppen, planen und überwachen.
- **pmrep.** Verwenden Sie `pmrep` zum Durchführen von Aufgaben zur Repository-Verwaltung, wie z. B. Auflisten von Repository-Objekten, Erstellen und Bearbeiten von Gruppen und Wiederherstellen und Löschen von Repositories.
- **mmcmd.** Verwenden Sie `mmcmd`, um Ressourcen zu laden und zu verwalten und Modelle und benutzerdefinierte Ressourcen zu importieren und exportieren.
- **mmLineageMigrator.** Verwenden Sie „`mmLineageMigrator`“ zum Migrieren von Verknüpfungsinformationen der Datenverlaufskontrolle nach dem Upgrade von Metadata Manager 9.6.x auf die aktuelle Version.



**Hinweis:** Da dieses Programm automatisch ausgeführt wird, führen Sie dieses Programm nicht aus, außer wenn die Migration fehlschlägt und Sie den Fehler beheben, oder wenn Sie durch den globalen Kundensupport von Informatica zum Ausführen dieses Programms angewiesen werden.

- **mmRepoCmd.** Verwenden Sie mmRepoCmd, um Metadata Manager-Repository-Inhalte zu erstellen, zu löschen, zu sichern und wiederherzustellen. Sie können auch eine PowerCenter-Repository-Sicherungsdatei, die Metadata Manager-Objekte enthält, in der PowerCenter-Repository-Datenbank wiederherstellen.
- **mmXConPluginUtil.** Verwenden Sie „mmXConPluginUtil“ zum Generieren der Bild-Mapping-Informationen oder des Plug-Ins für ein universelles XConnect.
- **rcfmu.** Migrieren Sie eine Ressourcenkonfigurationsdatei aus einer früheren Version von Metadata Manager auf die aktuelle Version mit „rcfmu“.
- **rmu.** Migrieren Sie Ressourcen aus einer früheren Version von Metadata Manager auf die aktuelle Version mit „rmu“.

Zum Ausführen von Befehlszeilenprogrammen unter UNIX müssen Sie ggf. die Bibliothekspfad-Umgebungsvariable auf den Speicherort der Informatica-Dienstprogramme festlegen.

Um die Bedienbarkeit zu erleichtern, können Sie Umgebungsvariablen konfigurieren, die bei jeder Ausführung der Befehlszeilenprogramme angewendet werden.

Sie können beispielsweise eine Umgebungsvariable für den Standarddomännennamen, den Benutzer und das Passwort festlegen, damit die Optionen nicht an der Befehlszeile eingegeben werden müssen.

## Eingeben von Optionen und Argumenten

Jedes Befehlszeilenprogramm erfordert eine Reihe von Optionen und Argumenten. Diese umfassen Benutzername, Passwort, Domänenname und Verbindungsinformationen.

Verwenden Sie beim Eingeben von Befehlsoptionen und -argumenten die folgenden Regeln:

- Geben Sie Optionen ein, indem Sie je nach der Programmsyntax für den Befehl einen Bindestrich gefolgt von einem Buchstaben, zwei Buchstaben oder einem Wort eingeben.  
Zum Beispiel verwendet der pmrep Connect-Befehl eine Option mit einem einzelnen Buchstaben für den Repository-Namen:

```
Connect -r <repository_name>
```

- Geben Sie Optionen in beliebiger Reihenfolge ein.
- Wenn eine von Ihnen über die Befehlszeile angegebene Option Leerzeichen enthält, setzen Sie die Option in doppelte Anführungszeichen.
- Das erste Wort nach der Option ist das Argument.
- Die meisten Optionen erfordern Argumente.  
Bei Verwendung von pmcmd oder infacmd müssen Sie Optionen von Argumenten mit einem einzelnen Leerzeichen trennen. Wenn Sie pmrep verwenden, müssen Sie Optionen nicht von Argumenten trennen.
- Wenn ein Argument mehr als ein Wort enthält, setzen Sie das Argument in doppelte Anführungszeichen. Für „pmrep“ und „pmcmd“ können Sie auch einfache Anführungszeichen verwenden.

Unpaarige Anführungszeichen führen zu einem Fehler.

Für „infacmd“ oder „pmcmd“ ignorieren die Befehlszeilenprogramme Anführungszeichen, die kein Argument umschließen.

- Wenn ein Argument im Format `optionsname=wert` vorliegt und der Wert sowohl ein Leerzeichen als auch ein Gleichheitszeichen (=) enthält, muss dem Gleichheitszeichen ein umgekehrter Schrägstrich vorangestellt werden.  
Beispiel: Ein Argument enthält die Option `DatabaseUser`, und der Name des Datenbankbenutzers lautet `a#v%5^=! !`. Verwenden Sie bei Eingabe des Arguments das folgende Format: `DBUser=a#v%5^!\=!`
- Um die Verbindungsoptionen mit vorhandenen Umgebungsvariablen zu aktualisieren, geben Sie in allen Shells außer `csh` vor jedem Dollarzeichen (\$) ein Escapezeichen ein.
- Für „`pmcmd`“ können Sie Leerzeichen in einem Argument verwenden. Um ein Argument mit Leerzeichen anzugeben, schließen Sie das Argument in einfache oder doppelte Anführungszeichen ein. Wenn Sie einfache oder doppelte Anführungszeichen im Argument verwenden, muss ihnen ein umgekehrter Schrägstrich vorangestellt werden.

## Syntax-Notation

In der folgenden Tabelle wird die in diesem Buch zur Angabe der Syntax für alle Informatica-Befehlszeilenprogramme verwendete Notation beschrieben:

Konvention	Beschreibung
-x	Eine vor einem Argument platzierte Option. Diese kennzeichnet den Parameter, den Sie eingeben. Um z. B. den Benutzernamen für <code>pmcmd</code> einzugeben, geben Sie <code>-u</code> oder <code>-user</code> gefolgt vom Benutzernamen ein.
< x >	Erforderliche Option. Wenn Sie eine erforderliche Option nicht angeben, gibt das Befehlszeilenprogramm eine Fehlermeldung zurück.
<x   y >  {x   y}	Wählen Sie zwischen erforderlichen Optionen aus. Um den Befehl auszuführen, müssen Sie aus den aufgeführten Optionen auswählen. Wenn Sie eine erforderliche Option nicht angeben, gibt das Befehlszeilenprogramm eine Fehlermeldung zurück. In <code>pmrep</code> kennzeichnen die geschweiften Klammern Gruppen von erforderlichen Optionen, wie im folgenden Beispiel:  <pre>KillUserConnection {-i &lt;connection_id&gt;    -n &lt;user_name&gt;    -a (kill all)}</pre> Wenn ein Pipesymbol ( ) Optionen trennt, müssen Sie genau eine Option angeben. Wenn Optionen nicht durch Pipesymbole getrennt sind, müssen Sie alle Optionen angeben.
[ x ]	Optionaler Parameter. Der Befehl wird unabhängig von der Eingabe optionaler Parameter ausgeführt. Zum Beispiel hat der <code>Help</code> -Befehl die folgende Syntax:  <pre>Help [Command]</pre> Wenn Sie einen Befehl eingeben, gibt das Befehlszeilenprogramm Informationen nur zu diesem Befehl zurück. Wenn Sie den Namen des Befehls nicht angeben, gibt das Befehlszeilenprogramm eine Liste aller Befehle zurück.

Konvention	Beschreibung
[ x   y ]	<p>Wählen Sie zwischen optionalen Parametern aus.</p> <p>Viele Befehle in pmcmd werden beispielsweise entweder im Warte- oder im Nichtwarte-Modus ausgeführt.</p> <p>[ -wait   -nowait ]</p> <p>Wenn Sie einen Modus angeben, wird der Befehl im angegebenen Modus ausgeführt. Der Befehl wird unabhängig von der Eingabe des optionalen Parameters ausgeführt.</p> <p>Wenn Sie keinen Modus angeben, führt pmcmd den Befehl im standardmäßigen Nichtwarte-Modus aus.</p>
< < x   y >   < a   b > >	<p>Wenn ein Satz eine Teilmenge enthält, wird die Obermenge mit Klammern in Fettschrift &lt; &gt; angegeben.</p> <p>Ein Pipesymbol in Fettschrift (   ) trennt die Teilmengen.</p>
(Text)	<p>In pmrep wird beschreibender Text von Parenthesen umschlossen. Hierzu gehören beispielsweise die Liste möglicher Werte für ein Argument oder eine Erläuterung zu einer Option, die kein Argument annimmt.</p>

## Ausführen von Befehlen in einer sicheren Domäne

Wenn für die Informatica-Domäne die sichere Kommunikation aktiviert ist, müssen Sie Umgebungsvariablen auf dem Rechner setzen, auf dem sich die Befehlszeilenprogramme zum sicheren Ausführen der Befehle befinden. Sie müssen die Umgebungsvariablen vor dem Ausführen der Befehle „infacmd“, „pmrep“, „mmcmd“, „mmRepoCmd“ und „pmcmd“ setzen.

Setzen Sie die folgenden Umgebungsvariablen vor dem Ausführen der Befehle fest:

### INFA\_TRUSTSTORE

Setzen Sie die Umgebungsvariable INFA\_TRUSTSTORE auf das Verzeichnis, das die Truststore-Dateien für die SSL-Zertifikate enthält. Das Verzeichnis muss Truststore-Dateien mit der Bezeichnung „infa\_truststore.jks“ und „infa\_truststore.pem“ enthalten. Sie müssen die INFA\_TRUSTSTORE-Variable setzen, egal ob Sie das Standard-SSL-Zertifikat von Informatica verwenden oder ein SSL-Zertifikat angeben.

### INFA\_TRUSTSTORE\_PASSWORD

Wenn Sie das SSL-Zertifikat angeben, um die sichere Kommunikation in der Domäne zu aktivieren, setzen Sie die Umgebungsvariable INFA\_TRUSTSTORE\_PASSWORD auf das Passwort für die Datei infa\_truststore.jks, die das SSL-Zertifikat enthält. Sie brauchen diese Variable nicht zu setzen, wenn Sie das Standard-SSL-Zertifikat von Informatica verwenden.

**Hinweis:** Das Passwort muss verschlüsselt werden. Verwenden Sie das Befehlszeilenprogramm pmpasswd zum Verschlüsseln des Passworts mit Verschlüsselungstyp CRYPT\_SYSTEM. Weitere Informationen hierzu finden Sie unter [“Encrypting Passwords” auf Seite 61](#).

# Ausführen von Befehlen unter UNIX mit Kerberos-Authentifizierung

Wenn die Informatica-Domäne Kerberos-Authentifizierung verwendet, setzen Sie die Umgebungsvariable der Kerberos-Konfiguration vor dem Ausführen der Befehlszeilenprogramme. Wenn Sie die Befehlszeilenprogramme mit Single Sign-On ausführen, müssen Sie eine Cache-Datei für Anmeldedaten generieren und den Pfad und Dateinamen in einer Umgebungsvariable angeben.

Sie müssen die Umgebungsvariablen vor dem Ausführen der Befehle „infacmd“, „pmrep“, „mmcmd“, „mmRepoCmd“ und „pmcmd“ unter UNIX setzen.

## Ausführen von Befehlen unter UNIX mit Single Sign On

Wenn Sie die Befehlszeilenprogramme mit Single Sign-On ausführen, müssen Sie eine Cache-Datei für Anmeldedaten generieren, um das Benutzerkonto, das die Befehle im Kerberos-Netzwerk ausführt, zu authentifizieren. Verwenden Sie das Dienstprogramm *kinit* zum Generieren der Cache-Datei für Anmeldedaten.

Wenn Sie über eine Cache-Datei für Anmeldedaten verfügen, können Sie die Befehle ohne die Optionen für Benutzername und Passwort ausführen.

Um Befehle unter UNIX mit den Single Sign On auszuführen, führen Sie folgende Aufgaben durch:

1. Setzen Sie die Kerberos-Umgebungsvariablen.
2. Laden Sie das Dienstprogramm *kinit* herunter und generieren Sie eine Cache-Datei für Anmeldedaten.

## Einstellen der Kerberos-Umgebungsvariablen

Auf dem Rechner, auf dem sich die Befehlszeilenprogramme befinden, geben Sie den Speicherort des Anmeldedaten-Caches und der Konfigurationsdatei in den Kerberos-Umgebungsvariablen an.

Richten Sie die folgenden Umgebungsvariablen ein:

### **KRB5CCNAME**

Speichert den Standardpfad und -dateinamen für den Kerberos-Anmeldedaten-Cache. Wenn Sie das Dienstprogramm *kinit* zum Generieren des Caches für Benutzeranmeldedaten verwenden, speichert *kinit* den Anmeldedaten-Cache in der Standarddatei, die Sie in der Umgebungsvariable KRB5CCNAME festgelegt haben.

### **KRB5\_CONFIG**

Speichert den Pfad und den Dateinamen der Kerberos-Konfigurationsdatei. Der Name der Kerberos-Konfigurationsdatei lautet *krb5.conf*. Weitere Informationen über den Inhalt der Datei *krb5.conf* finden Sie im *Informatica Sicherheitshandbuch*.

## Generieren der Cache-Datei für Anmeldedaten

Verwenden Sie das Kerberos-Dienstprogramm *kinit*, um die Cache-Datei mit den Anmeldedaten für das Benutzerkonto zu generieren, das die Befehlszeilenprogramme ausführt. Das Dienstprogramm ist im Download-Paket von MIT Kerberos V5 verfügbar.

Führen Sie zum Generieren der Cache-Datei mit den Anmeldedaten folgende Aufgaben durch:

1. Laden Sie MIT Kerberos V5 herunter und installieren Sie es.

Sie können MIT Kerberos V5 von folgender Website herunterladen: <http://web.mit.edu/Kerberos/dist/#krb5-1.12>

2. Führen Sie das Dienstprogramm *kinit* aus und geben Sie den Benutzerprinzipalnamen ein.

Beim Erstellen des Caches für Benutzeranmeldedaten müssen Sie die Option „forwardable“ (-f) verwenden. Sie können die folgende Befehlssyntax verwenden:

```
kinit -f <Prinzipalname>
```

Das Format für den Prinzipalnamen ist <Benutzername>@<Bereichsname.com>. Geben Sie den Bereichsnamen in Großbuchstaben ein.

**Hinweis:** Wenn Sie die Umgebungsvariable *KRB5CCNAME* festlegen, bevor Sie das Dienstprogramm *kinit* ausführen, speichert *kinit* den Anmeldedaten-Cache an dem Speicherort, der in der Umgebungsvariable angegeben ist.

3. Geben Sie das Passwort für das Benutzerkonto ein.

## Ausführen von Befehlen unter UNIX ohne Single Sign On

Um Befehle unter UNIX ohne Single Sign On auszuführen, setzen Sie die Umgebungsvariable *KRB5\_CONFIG* auf den Pfad und den Dateinamen der Kerberos-Konfigurationsdatei. Schließen Sie den Benutzernamen und das Passwort ein, wenn Sie den Befehl ausführen, oder setzen Sie den Benutzernamen und das Passwort in Umgebungsvariablen.

Die Befehle bestimmen die Benutzeranmeldedaten, je nachdem, wie Sie den Benutzernamen und das Passwort angeben. Die Befehle prüfen die Anmeldedaten in folgender Reihenfolge:

1. Befehlsoptionen. Wenn Sie die Benutzernamenoption („-un“) und die Passwortoption („-pd“) in den Befehl einbeziehen, verwendet der Befehl den Benutzernamen und das Passwort, die für die Optionen angegeben sind.

Wenn die Domäne einen einzelnen Kerberos-Bereich für die Authentifizierung verwendet, geben Sie den SAM-Kontonamen für den Benutzer als Wert für die Benutzernamenoption an. Wenn die Domäne die bereichsübergreifende Kerberos-Authentifizierung verwendet, geben Sie den Benutzerprinzipalnamen als Wert für die Benutzernamenoption an.

2. Umgebungsvariablen. Wenn Sie die Benutzernamenoption und die Passwortoption in den Befehl nicht einbeziehen, verwendet der Befehl den Benutzernamen und das Passwort, die in den Umgebungsvariablen *INFA\_DEFAULT\_DOMAIN\_USER* und *INFA\_DEFAULT\_DOMAIN\_PASSWORD* angegeben sind.

**Hinweis:** Wenn Sie die Anmeldedaten nicht in den Befehlsoptionen oder Umgebungsvariablen setzen, sucht der Befehl nach einer Cache-Datei für Anmeldedaten. Wenn ein Anmeldedaten-Cache verfügbar ist, wird der Befehl mit Single Sign On ausgeführt.

## Ausführen von Befehlen unter Windows mit Kerberos-Authentifizierung

Unter Windows verwenden die Befehle „*infacmd*“, „*pmrep*“, „*mmcmd*“, „*mmRepoCmd*“ und „*pmcmd*“ die eingegebenen Anmeldedaten für Single Sign-On. Sie müssen keine Cach-Datei für Anmeldedaten generieren.

Wenn Sie Single Sign-On nicht unter Windows verwenden, legen Sie die Umgebungsvariable *KRB5\_CONFIG* auf den Pfad und den Dateinamen der Kerberos-Konfigurationsdatei fest. Der Name der Konfigurationsdatei lautet *krb5.conf*.

Die Befehle bestimmen die Benutzeranmeldedaten, je nachdem, wie Sie den Benutzernamen und das Passwort angeben. Die Befehle prüfen die Anmeldedaten in folgender Reihenfolge:

1. Befehlsoptionen. Wenn Sie die Benutzernamenoption („-un“) und die Passwortoption („-pd“) in den Befehl einbeziehen, verwendet der Befehl den Benutzernamen und das Passwort, die für die Optionen angegeben sind.

Wenn die Domäne einen einzelnen Kerberos-Bereich für die Authentifizierung verwendet, geben Sie den SAM-Kontonamen für den Benutzer als Wert für die Benutzernamenoption an. Wenn die Domäne die bereichsübergreifende Kerberos-Authentifizierung verwendet, geben Sie den Benutzerprinzipalnamen als Wert für die Benutzernamenoption an.

2. Umgebungsvariablen. Wenn Sie die Benutzernamenoption und die Passwortoption in den Befehl nicht einbeziehen, verwendet der Befehl den Benutzernamen und das Passwort, die in den Umgebungsvariablen INFA\_DEFAULT\_DOMAIN\_USER und INFA\_DEFAULT\_DOMAIN\_PASSWORD angegeben sind.

**Hinweis:** Wenn Sie die Anmeldedaten in den Befehlsoptionen oder Umgebungsvariablen nicht setzen, verwendet der Befehl die eingegebenen Anmeldedaten und führt den Befehl mit Single Sign On aus.

# KAPITEL 4

## Umgebungsvariablen für Befehlszeilenprogramme

Dieses Kapitel umfasst die folgenden Themen:

- [Umgebungsvariablen für Befehlszeilenprogramme - Übersicht, 44](#)
- [ICMD\\_JAVA\\_OPTS, 45](#)
- [INFA\\_CLIENT\\_RESILIENCE\\_TIMEOUT, 46](#)
- [INFA\\_CODEPAGENAME, 47](#)
- [INFA\\_DEFAULT\\_DATABASE\\_PASSWORD, 47](#)
- [INFA\\_DEFAULT\\_DB\\_TRUSTSTORE\\_PASSWORD, 49](#)
- [INFA\\_DEFAULT\\_DOMAIN, 50](#)
- [INFA\\_DEFAULT\\_DOMAIN\\_PASSWORD, 50](#)
- [INFA\\_DEFAULT\\_DOMAIN\\_USER, 51](#)
- [INFA\\_DEFAULT\\_PWX\\_OSEPASSWORD, 52](#)
- [INFA\\_DEFAULT\\_PWX\\_OSPASSWORD, 53](#)
- [INFA\\_DEFAULT\\_SECURITY\\_DOMAIN, 53](#)
- [INFA\\_DOMAINS\\_FILE, 54](#)
- [INFA\\_JAVA\\_CMD\\_OPTS, 55](#)
- [INFA\\_PASSWORD, 55](#)
- [INFA\\_NODE\\_KEYSTORE\\_PASSWORD, 57](#)
- [INFA\\_NODE\\_TRUSTSTORE\\_PASSWORD, 58](#)
- [INFA\\_REPCNX\\_INFO, 58](#)
- [INFA\\_REPOSITORY\\_PASSWORD, 59](#)
- [INFATool\\_DATEFORMAT, 60](#)
- [Encrypting Passwords, 61](#)
- [Festlegen des Benutzernamens, 62](#)

# Umgebungsvariablen für Befehlszeilenprogramme - Übersicht

Sie können optionale Umgebungsvariablen für die Befehlszeilenprogramme konfigurieren. Sie können beispielsweise Umgebungsvariablen verwenden, um Passwörter zu verschlüsseln, Anzeigeoptionen für Uhrzeit und Datum zu konfigurieren und die Standardanmeldeinformationen für eine Domäne zu speichern.

Wenn Sie `pmcmd` oder `pmrep` im interaktiven Modus ausführen, müssen Sie das Befehlszeilenprogramm beenden und anschließend erneut aufrufen, um die geänderten Umgebungsvariablen zu verwenden.

Unter Windows können Sie diese Umgebungsvariablen entweder als Benutzer- oder Systemvariablen konfigurieren. Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

**Hinweis:** Die von Ihnen konfigurierten Umgebungsvariablen gelten für Befehlszeilenprogramme, auf dem Knoten ausgeführt werden. Starten Sie den Knoten neu, damit die Änderungen wirksam werden.

In der folgenden Tabelle werden die Umgebungsvariablen beschrieben, die Sie zur Verwendung mit den Befehlszeilenprogrammen konfigurieren können:

Umgebungsvariable	Befehlszeilenprogramme	Beschreibung
ICMD_JAVA_OPTS	infacmd	Legt Java-Optionen fest.
INFA_CLIENT_RESILIENCE_TIMEOUT	infacmd pmcmd pmrep	Begrenzt die Anzahl der Sekunden, die für die Befehlszeilenprogramme zum Herstellen einer Verbindung zur Domäne oder zum Dienst zulässig sind.
INFA_CODEPAGENAME	pmcmd pmrep	Konfiguriert den Zeichensatz <i>pmcmd</i> und die Verwendung von <i>pmrep</i> .
INFA_DEFAULT_CONNECTION_PASSWORD	infacmd	Speichert das Passwort der Datenbank-Truststore-Datei für die sichere Datenbank.
INFA_DEFAULT_DATABASE_PASSWORD	infasetup Rückgabewerte	Speichert das Benutzernamen-Standardpasswort für die Domänenkonfigurations-Datenbank.
INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD	infasetup Rückgabewerte	Speichert das Datenbank-Truststore-Passwort.
INFA_DEFAULT_DOMAIN	infacmd pmcmd pmrep	Speichert den Standarddomännennamen.
INFA_DEFAULT_DOMAIN_PASSWORD	infacmd	Speichert das Benutzernamen-Standardpasswort für die Domäne.
INFA_DEFAULT_DOMAIN_USER	infacmd	Speichert den Benutzernamen für die Domäne.
INFA_DEFAULT_PWX_OSEPASSWORD	infacmd pwX	Speichert ein verschlüsseltes Passwort für das Betriebssystem.



Umgebungsvariable	Befehlszeilenprogramme	Beschreibung
INFA_DEFAULT_PWX_OSPASSWORD	infacmd pwx	Speichert ein Nur-Text-Passwort für das Betriebssystem.
INFA_DEFAULT_SECURITY_DOMAIN	infacmd	Speichert die Sicherheitsdomäne für die LDAP-Authentifizierung.
INFA_DOMAINS_FILE	infacmd infasetup Rückgabewerte pmcmd pmrep	Speichert den Pfad und den Namen der Datei „domains.infa“.
INFA_JAVA_CMD_OPTS	infasetup Rückgabewerte	Legt Java-Optionen fest.
INFA_NODE_KEYSTORE_PASSWORD	infasetup Rückgabewerte	Speichert das Passwort für die Datei „infa_keystore.jks“.
INFA_NODE_TRUSTSTORE_PASSWORD	infasetup Rückgabewerte	Speichert das Passwort für die Datei „infa_truststore.jks“.
INFA_PASSWORD	infacmd	Speichert das Standardpasswort für den Benutzer.
INFA_REPCNX_INFO	pmrep	Speichert die Namen der Repository-Verbindungsdatei.
INFA_REPOSITORY_PASSWORD	infacmd	Speichert das PowerCenter-Repository-Standardpasswort für den Benutzer.
INFATool_DATEFORMAT	pmcmd	Konfiguriert die Art und Weise, wie pmcmd das Datum und die Uhrzeit anzeigt.
<Password_Environment_Variable>	pmcmd pmrep	Verschlüsselt und speichert das Passwort.
<User_Name_Environment_Variable>	pmcmd pmrep	Speichert den Benutzernamen.

#### VERWANDTE THEMEN:

- [“Encrypting Passwords” auf Seite 61](#)
- [“Festlegen des Benutzernamens” auf Seite 62](#)

## ICMD\_JAVA\_OPTS

Die ICMD\_JAVA\_OPTS-Umgebungsvariable gilt für das infacmd-Befehlszeilenprogramm.

Sie können die Umgebungsvariable ICMD\_JAVA\_OPTS konfigurieren, um die Java-Optionen wie zum Beispiel -Xmx-Werte und Systemeigenschaften festzulegen. Leiten Sie zum Festlegen einer Systemeigenschaft den Wert in folgendem Format weiter:

```
-Dproperty.name=property.value
```

Sie möchten beispielsweise den von infacmd verwendeten Systemspeicher erhöhen. Der Standardwert für den infacmd-Systemspeicher beträgt 512 MB. Geben Sie zum Konfigurieren von 1024 MB Systemspeicher in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv ICMD_JAVA_OPTS "-Xmx1024m"
```

## Konfigurieren von ICMD\_JAVA\_OPTS unter UNIX

So konfigurieren Sie ICMD\_JAVA\_OPTS unter UNIX:

- Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv ICMD_JAVA_OPTS <Java_Options>
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
ICMD_JAVA_OPTS = <Java_Options>  
export ICMD_JAVA_OPTS
```

## Konfigurieren von ICMD\_JAVA\_OPTS unter Windows

So konfigurieren Sie ICMD\_JAVA\_OPTS unter Windows:

- Geben Sie die Umgebungsvariable ICMD\_JAVA\_OPTS ein und legen Sie die Java-Optionen wie die -Xmx-Werte und Systemeigenschaften fest.

Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

# INFA\_CLIENT\_RESILIENCE\_TIMEOUT

Die INFA\_CLIENT\_RESILIENCE\_TIMEOUT-Umgebungsvariable gilt für das infacmd-, pmcmd- und pmrep-Befehlszeilenprogramm.

Sie können die Umgebungsvariable INFA\_CLIENT\_RESILIENCE\_TIMEOUT so festlegen, dass die Anzahl der Sekunden begrenzt wird, die für die Befehlszeilenprogramme zum Herstellen einer Verbindung zur Domäne oder zum Dienst zulässig sind. Der Standardwert beträgt 180 Sekunden, wenn Sie diese Umgebungsvariable nicht festlegen.

## Konfigurieren von INFA\_CLIENT\_RESILIENCE\_TIMEOUT unter UNIX

So konfigurieren Sie INFA\_CLIENT\_RESILIENCE\_TIMEOUT unter UNIX:

- Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv INFA_CLIENT_RESILIENCE_TIMEOUT <number of seconds>
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
INFA_CLIENT_RESILIENCE_TIMEOUT = <number of seconds>  
export INFA_CLIENT_RESILIENCE_TIMEOUT
```

## Konfigurieren von INFA\_CLIENT\_RESILIENCE\_TIMEOUT unter Windows

So konfigurieren Sie INFA\_CLIENT\_RESILIENCE\_TIMEOUT unter Windows:

- Geben Sie die Umgebungsvariable INFA\_CLIENT\_RESILIENCE\_TIMEOUT ein und wählen Sie einen Wert für die Anzahl der Sekunden aus, der für die Befehlszeilenprogramme zum Herstellen einer Verbindung zur Domäne oder zum Dienst zulässig ist.

Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

## INFA\_CODEPAGE\_NAME

Die INFA\_CODEPAGE\_NAME-Umgebungsvariable gilt für das pmcmd- und pmrep-Befehlszeilenprogramm.

*pmcmd* und *pmrep* senden Befehle im Unicode-Format und verwenden die Codeseite des Host-Rechners, es sei denn, Sie legen die Codeseiten-Umgebungsvariable INFA\_CODEPAGE\_NAME fest, um sie zu überschreiben. Wenn Sie INFA\_CODEPAGE\_NAME für *pmcmd* festlegen, muss die Codeseite mit der Integration Service-Codeseite kompatibel sein. Wenn Sie INFA\_CODEPAGE\_NAME für *pmrep* festlegen, muss die Codeseite mit der Repository-Codeseite kompatibel sein. Wenn Sie INFA\_CODEPAGE\_NAME auf dem Rechner festlegen, auf dem Sie *pmcmd* und *pmrep* ausführen, muss die Codeseite mit den Integration Service- und Repository-Codeseiten kompatibel sein.

Wenn die Codeseiten nicht kompatibel sind, schlägt der Befehl möglicherweise fehl.

## Konfigurieren von INFA\_CODEPAGE\_NAME unter UNIX

So konfigurieren Sie INFA\_CODEPAGE\_NAME unter UNIX:

- Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv INFA_CODEPAGE_NAME <code page name>
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
INFA_CODEPAGE_NAME = <code page name>  
export INFA_CODEPAGE_NAME
```

## Konfigurieren von INFA\_CODEPAGE\_NAME unter Windows

So konfigurieren Sie INFA\_CODEPAGE\_NAME unter Windows:

- Geben Sie die Umgebungsvariable INFA\_CODEPAGE\_NAME ein und legen Sie den Namen der Codeseite als Wert fest.

Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

## INFA\_DEFAULT\_DATABASE\_PASSWORD

Die INFA\_DEFAULT\_DATABASE\_PASSWORD-Umgebungsvariable gilt für das infasetup-Befehlszeilenprogramm.

Für einige *infasetup*-Befehle ist ein Domänen-Konfigurationsdatenbank-Passwort erforderlich. Sie können dieses Passwort als Option mit *infasetup* bereitstellen oder als Umgebungsvariable `INFA_DEFAULT_DATABASE_PASSWORD` speichern.

Verwenden Sie die folgenden Schritte als Richtlinie zur Verwendung eines verschlüsselten Passworts als eine Umgebungsvariable:

1. Verwenden Sie das Befehlszeilenprogramm *pmpasswd* zum Verschlüsseln des Datenbankbenutzerpassworts.  
*pmpasswd* generiert und zeigt das verschlüsselte Passwort an. Wenn Sie beispielsweise das Passwort "monday" eingeben, wird dieses wie folgt verschlüsselt: f/wRb5PZsZnqESTDPeos7Q==.
2. Konfigurieren Sie die Passwortumgebungsvariable, um den verschlüsselten Wert festzulegen.

### VERWANDTE THEMEN:

- ["Encrypting Passwords" auf Seite 61](#)

## Konfigurieren von `INFA_DEFAULT_DATABASE_PASSWORD` unter UNIX

So konfigurieren Sie `INFA_DEFAULT_DATABASE_PASSWORD` unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:  

```
pmpasswd <database password>
```

*pmpasswd* gibt das verschlüsselte Passwort zurück.
2. Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:  

```
setenv INFA_DEFAULT_DATABASE_PASSWORD <encrypted password>
```

  
Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:  

```
INFA_DEFAULT_DATABASE_PASSWORD = <encrypted password>
export INFA_DEFAULT_DATABASE_PASSWORD
```

## Konfigurieren von `INFA_DEFAULT_DATABASE_PASSWORD` unter Windows

So konfigurieren Sie `INFA_DEFAULT_DATABASE_PASSWORD` unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:  

```
pmpasswd <database password>
```

*pmpasswd* gibt das verschlüsselte Passwort zurück.
2. Geben Sie die Umgebungsvariable `INFA_DEFAULT_DATABASE_PASSWORD` ein und legen Sie das verschlüsselte Passwort als Wert fest.  
  
Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

# INFA\_DEFAULT\_DB\_TRUSTSTORE\_PASSWORD

Die Umgebungsvariable `INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD` gilt für das `infasetup`-Befehlszeilenprogramm.

Einige `infasetup`-Befehle konfigurieren die sichere Kommunikation für die Domäne. Sie können das Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank als Option mit `infasetup` angeben, oder Sie können es als Umgebungsvariable `INFA_DEFAULT_DB_TRUSTSTORE_DATABASE_PASSWORD` speichern.

Verwenden Sie die folgenden Schritte als Richtlinie zur Verwendung eines verschlüsselten Passworts als eine Umgebungsvariable:

1. Verwenden Sie das Befehlszeilenprogramm `pmpasswd` zum Verschlüsseln des Datenbankbenutzerpassworts.

`pmpasswd` generiert und zeigt das verschlüsselte Passwort an. Wenn Sie beispielsweise das Passwort „monday“ eingeben, wird dieses wie folgt verschlüsselt: `f/wRb5PZsZnqESTDPeos7Q==`.

2. Konfigurieren Sie die Passwortumgebungsvariable, um den verschlüsselten Wert festzulegen.

## Konfigurieren von INFA\_DEFAULT\_DB\_TRUSTSTORE\_PASSWORD unter UNIX

So konfigurieren Sie `INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD` unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:

```
pmpasswd <database password>
```

`pmpasswd` gibt das verschlüsselte Passwort zurück.

2. Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD <encrypted password>
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD = <encrypted password>
export INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD
```

## Konfigurieren von INFA\_DEFAULT\_DB\_TRUSTSTORE\_PASSWORD unter Windows

So konfigurieren Sie `INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD` unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:

```
pmpasswd <database password>
```

`pmpasswd` gibt das verschlüsselte Passwort zurück.

2. Geben Sie die Umgebungsvariable `INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD` ein und legen Sie das verschlüsselte Passwort als Wert fest.

Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

# INFA\_DEFAULT\_DOMAIN

Die INFA\_DEFAULT\_DOMAIN-Umgebungsvariable gilt für das `infacmd`-, `pmcmd`- und `pmrep`-Befehlszeilenprogramm.

Für die Befehlszeilenprogramme ist ein Domänenname erforderlich. Sie können den Domännennamen als eine Option mit den Befehlszeilenprogrammen bereitstellen oder ihn als Umgebungsvariable `INFA_DEFAULT_DOMAIN` speichern. Wenn Sie mehr als eine Domäne haben, wählen Sie eine Standarddomäne aus.

## Konfigurieren von INFA\_DEFAULT\_DOMAIN unter UNIX

So konfigurieren Sie `INFA_DEFAULT_DOMAIN` unter UNIX:

- Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv INFA_DEFAULT_DOMAIN <domain name>
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
INFA_DEFAULT_DOMAIN = <domain name>  
export INFA_DEFAULT_DOMAIN
```

## Konfigurieren von INFA\_DEFAULT\_DOMAIN unter Windows

So konfigurieren Sie `INFA_DEFAULT_DOMAIN` unter Windows:

- Geben Sie die Umgebungsvariable `INFA_DEFAULT_DOMAIN` ein und legen Sie den Domännennamen als Wert fest.

Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

# INFA\_DEFAULT\_DOMAIN\_PASSWORD

Die `INFA_DEFAULT_DOMAIN_PASSWORD`-Umgebungsvariable gilt für das `infacmd`-Befehlszeilenprogramm.

Für die meisten `infacmd`-Befehle ist ein Benutzerpasswort erforderlich. Sie können ein Benutzerpasswort als Option mit `infacmd` bereitstellen oder als Umgebungsvariable `INFA_DEFAULT_DOMAIN_PASSWORD` speichern.

Verwenden Sie die folgenden Schritte als Richtlinie zur Verwendung eines verschlüsselten Passworts als eine Umgebungsvariable:

1. Verwenden Sie das Befehlszeilenprogramm `pmpasswd` zum Verschlüsseln des Benutzerpassworts.  
`pmpasswd` generiert und zeigt das verschlüsselte Passwort an. Wenn Sie beispielsweise das Passwort "monday" eingeben, wird dieses wie folgt verschlüsselt: `f/wRb5PZsZnqESTDPeos7Q==`.
2. Konfigurieren Sie die Passwortumgebungsvariable, um den verschlüsselten Wert festzulegen.

## VERWANDTE THEMEN:

- [“Encrypting Passwords” auf Seite 61](#)

## Konfigurieren von INFA\_DEFAULT\_DOMAIN\_PASSWORD unter UNIX

So konfigurieren Sie INFA\_DEFAULT\_DOMAIN\_PASSWORD unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:

```
mpasswd <password>
```

*mpasswd* gibt das verschlüsselte Passwort zurück.

2. Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv INFA_DEFAULT_DOMAIN_PASSWORD <encrypted password>
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
INFA_DEFAULT_DOMAIN_PASSWORD = <encrypted password>
export INFA_DEFAULT_DOMAIN_PASSWORD
```

## Konfigurieren von INFA\_DEFAULT\_DOMAIN\_PASSWORD unter Windows

So konfigurieren Sie INFA\_DEFAULT\_DOMAIN\_PASSWORD unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:

```
mpasswd <password>
```

*mpasswd* gibt das verschlüsselte Passwort zurück.

2. Geben Sie die Umgebungsvariable INFA\_DEFAULT\_DOMAIN\_PASSWORD ein und legen Sie das *verschlüsselte* Passwort als Wert fest.

Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

## INFA\_DEFAULT\_DOMAIN\_USER

Die INFA\_DEFAULT\_DOMAIN\_USER-Umgebungsvariable gilt für das *infacmd*-Befehlszeilenprogramm.

Für die meisten *infacmd*-Befehle ist ein Benutzername erforderlich. Sie können einen Benutzernamen als eine Option mit *infacmd* bereitstellen oder es als Umgebungsvariable INFA\_DEFAULT\_DOMAIN\_USER speichern.

## Konfigurieren von INFA\_DEFAULT\_DOMAIN\_USER unter UNIX

So konfigurieren Sie INFA\_DEFAULT\_DOMAIN\_USER unter UNIX:

- Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv INFA_DEFAULT_DOMAIN_USER <user name>
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
INFA_DEFAULT_DOMAIN_USER = <user name>
export INFA_DEFAULT_DOMAIN_USER
```

## Konfigurieren von INFA\_DEFAULT\_DOMAIN\_USER unter Windows

So konfigurieren Sie INFA\_DEFAULT\_DOMAIN\_USER unter Windows:

- Geben Sie die Umgebungsvariable INFA\_DEFAULT\_DOMAIN\_USER ein und legen Sie den Standardbenutzernamen als Wert fest.

Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

## INFA\_DEFAULT\_PWX\_OSEPASSWORD

Die INFA\_DEFAULT\_PWX\_OSEPASSWORD- Umgebungsvariable gilt für das infacmd pwx-Befehlszeilenprogramm.

Für einige infacmd pwx-Befehle ist ein Betriebssystempasswort erforderlich. Sie können ein verschlüsseltes Passwort als eine Option mit infacmd pwx bereitstellen oder es als Umgebungsvariable INFA\_DEFAULT\_PWX\_OSEPASSWORD speichern.

Verwenden Sie die folgenden Schritte als Richtlinie zur Verwendung eines verschlüsselten Passworts als eine Umgebungsvariable:

1. Verwenden Sie zum Verschlüsseln des Passworts das pmpasswd-Befehlszeilenprogramm.  
Das pmpasswd-Programm generiert und zeigt das verschlüsselte Passwort an. Wenn Sie beispielsweise das Passwort "monday" eingeben, wird dieses wie folgt verschlüsselt: f/wRb5PZsZnqESTDPeos7Q==.
2. Konfigurieren Sie die Passwortumgebungsvariable, um den verschlüsselten Wert festzulegen.

### VERWANDTE THEMEN:

- ["Encrypting Passwords" auf Seite 61](#)

## Konfigurieren von INFA\_DEFAULT\_PWX\_OSEPASSWORD unter UNIX

So konfigurieren Sie INFA\_DEFAULT\_PWX\_OSEPASSWORD unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:

```
pmpasswd password
```

Das pmpasswd-Programm gibt das verschlüsselte Passwort zurück.

2. Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv INFA_DEFAULT_PWX_OSEPASSWORD encrypted_password
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
INFA_DEFAULT_PWX_OSEPASSWORD = encrypted_password  
export INFA_DEFAULT_PWX_OSEPASSWORD
```



## Konfigurieren von INFA\_DEFAULT\_PWX\_OSEPASSWORD unter Windows

So konfigurieren Sie INFA\_DEFAULT\_PWX\_OSEPASSWORD unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:

```
pmpasswd password
```

Das pmpasswd-Programm gibt das verschlüsselte Passwort zurück.

2. Geben Sie die Umgebungsvariable INFA\_DEFAULT\_PWX\_OSEPASSWORD ein und legen Sie das verschlüsselte Passwort als Wert fest.

Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

## INFA\_DEFAULT\_PWX\_OSPASSWORD

Die INFA\_DEFAULT\_PWX\_OSPASSWORD-Umgebungsvariable gilt für das infacmd pwx-Befehlszeilenprogramm.

Für einige infacmd pwx-Befehle ist ein Betriebssystempasswort erforderlich. Sie können ein Nur-Text-Passwort als Option mit infacmd pwx bereitstellen oder als Umgebungsvariable INFA\_DEFAULT\_PWX\_OSPASSWORD speichern.

## Konfigurieren von INFA\_DEFAULT\_PWX\_OSPASSWORD unter UNIX

So konfigurieren Sie INFA\_DEFAULT\_PWX\_OSPASSWORD unter UNIX:

- Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv INFA_DEFAULT_PWX_OSPASSWORD password
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
INFA_DEFAULT_PWX_OSPASSWORD = password  
export INFA_DEFAULT_PWX_OSPASSWORD
```

## Konfigurieren von INFA\_DEFAULT\_PWX\_OSPASSWORD unter Windows

Legen Sie zum Konfigurieren vom INFA\_DEFAULT\_PWX\_OSPASSWORD unter Windows das Nur-Text-Passwort als Wert fest.

Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

## INFA\_DEFAULT\_SECURITY\_DOMAIN

Die INFA\_DEFAULT\_SECURITY\_DOMAIN-Umgebungsvariable gilt für das infacmd-Befehlszeilenprogramm.

Für infacmd-Befehle ist eine Sicherheitsdomäne erforderlich, wenn Sie die LDAP-Authentifizierung verwenden und einen Informatica-Benutzer angeben. Sie können die Umgebungsvariable

INFA\_DEFAULT\_SECURITY\_DOMAIN für die native Sicherheitsdomäne oder für einen LDAP-Sicherheitsdomänennamen festlegen.

## Konfigurieren von INFA\_DEFAULT\_SECURITY\_DOMAIN unter UNIX

So konfigurieren Sie INFA\_DEFAULT\_SECURITY\_DOMAIN unter UNIX:

- Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv INFA_DEFAULT_SECURITY_DOMAIN <security domain name>
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
INFA_DEFAULT_SECURITY_DOMAIN = <security domain name>  
export INFA_DEFAULT_SECURITY_DOMAIN
```

## Konfigurieren von INFA\_DEFAULT\_SECURITY\_DOMAIN unter Windows

So konfigurieren Sie INFA\_DEFAULT\_SECURITY\_DOMAIN unter Windows:

- Geben Sie die Umgebungsvariable INFA\_DEFAULT\_SECURITY\_DOMAIN ein und legen Sie den Namen der Sicherheitsdomäne als Wert fest.

Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

# INFA\_DOMAINS\_FILE

Die INFA\_DOMAINS\_FILE-Umgebungsvariable gilt für die Befehlszeilenprogramme infacmd, infasetup, pmcmd und pmrep.

Wenn Sie die Informatica-Dienste mithilfe des Informatica-Installationsprogramms installieren, erstellt das Installationsprogramm eine Datei namens „domains.infa“ im Informatica-Installationsverzeichnis. Die Datei „domains.infa“ enthält die Konnektivitätsinformationen der Gateway-Knoten in einer Domäne, einschließlich Domänennamen, Domänenhostnamen und Domänenhost-Portnummern. Die Befehlszeilenprogramme benötigen die in der Datei „domains.infa“ enthaltenen Konnektivitätsinformationen, um eine Verbindung zu den Gateway-Knoten in einer Domäne herzustellen. Sie können die Umgebungsvariable INFA\_DOMAINS\_FILE auf den Pfad und den Namen der Datei „domains.infa“ setzen. Stellen Sie sicher, dass Sie die Variable INFA\_DOMAINS\_FILE auf dem Computer konfigurieren, auf dem die Informatica-Dienste installiert sind.

## Konfigurieren von INFA\_DOMAINS\_FILE unter UNIX

So konfigurieren Sie INFA\_DOMAINS\_FILE unter UNIX:

- Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv INFA_DOMAINS_FILE <file path><file name>
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
INFA_DOMAINS_FILE = <file path><file name>  
export INFA_DOMAINS_FILE
```

## Konfigurieren von INFA\_DOMAINS\_FILE unter Windows

So konfigurieren Sie INFA\_DOMAINS\_FILE unter Windows:

- Geben Sie die Umgebungsvariable INFA\_DOMAINS\_FILE ein und setzen Sie den Wert auf den Pfad und den Namen der Datei „domains.infa“.

Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

## INFA\_JAVA\_CMD\_OPTS

INFA\_JAVA\_CMD\_OPTS Umgebungsvariable gilt für das infasetup-Befehlszeilenprogramm.

Sie können die Umgebungsvariable INFA\_JAVA\_CMD\_OPTS konfigurieren, um die Java-Optionen wie zum Beispiel -Xmx-Werte und Systemeigenschaften festzulegen. Leiten Sie zum Festlegen einer Systemeigenschaft den Wert in folgendem Format weiter:

```
-Dproperty.name=property.value
```

Sie möchten beispielsweise den von infasetup verwendeten Systemspeicher erhöhen. Der Standardwert für den infasetup-Systemspeicher beträgt 512 MB. Geben Sie zum Konfigurieren von 1024 MB Systemspeicher in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv INFA_JAVA_CMD_OPTS "-Xmx1024m"
```

## Konfigurieren von INFA\_JAVA\_CMD\_OPTS unter UNIX

So konfigurieren Sie INFA\_JAVA\_CMD\_OPTS unter UNIX:

- Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv INFA_JAVA_CMD_OPTS <Java_Options>
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
INFA_JAVA_CMD_OPTS = <Java_Options>  
export INFA_JAVA_CMD_OPTS
```

## Konfigurieren von INFA\_JAVA\_CMD\_OPTS unter Windows

So konfigurieren Sie INFA\_JAVA\_CMD\_OPTS unter Windows:

- Geben Sie die Umgebungsvariable INFA\_JAVA\_CMD\_OPTS ein und legen Sie die Java-Optionen wie die -Xmx-Werte und Systemeigenschaften fest.

Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

## INFA\_PASSWORD

Die INFA\_PASSWORD-Umgebungsvariable gilt für das infacmd- und das infasetup-Befehlszeilenprogramm.

Für einige `infacmd`- und `infasetup`-Befehle ist ein Benutzerpasswort erforderlich. Sie können ein Benutzerpasswort als eine Option mit diesen Befehlen bereitstellen oder es als Umgebungsvariable `INFA_PASSWORD` speichern.

Sie können die Umgebungsvariable `INFA_PASSWORD` zum Speichern von unterschiedlichen Typen von Passwörtern verwenden. Im Befehl `infasetup DefineDomain` können Sie die Variable beispielsweise zum Festlegen des Schlüsselspeicherpassworts verwenden. Im Befehl `infacmd isp SetLDAPConnectivity` können Sie die Variable beispielsweise zum Festlegen des LDAP-Anmeldedatenpassworts verwenden. Möglicherweise müssen Sie den Wert der Variable basierend auf den von Ihnen ausgeführten Befehlen ändern.

Verwenden Sie die folgenden Schritte als Richtlinie zur Verwendung eines verschlüsselten Passworts als eine Umgebungsvariable:

1. Verwenden Sie das Befehlszeilenprogramm `mpasswd` zum Verschlüsseln des Benutzerpassworts.  
`mpasswd` generiert und zeigt das verschlüsselte Passwort an. Wenn Sie beispielsweise das Passwort "monday" eingeben, wird dieses wie folgt verschlüsselt: `f/wRb5PZsZnqESTDPeos7Q==`.
2. Konfigurieren Sie die Passwortumgebungsvariable, um den verschlüsselten Wert festzulegen.

### VERWANDTE THEMEN:

- ["Encrypting Passwords" auf Seite 61](#)

## Konfigurieren von `INFA_PASSWORD` unter UNIX

So konfigurieren Sie `INFA_PASSWORD` unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:  

```
mpasswd <password>
```

*mpasswd* gibt das verschlüsselte Passwort zurück.
2. Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv INFA_PASSWORD <encrypted password>
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
INFA_PASSWORD = <encrypted password>
export INFA_PASSWORD
```

## Konfigurieren von `INFA_PASSWORD` unter Windows

So konfigurieren Sie `INFA_PASSWORD` unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:  

```
mpasswd <password>
```

*mpasswd* gibt das verschlüsselte Passwort zurück.
2. Geben Sie die Umgebungsvariable `INFA_PASSWORD` ein und legen Sie das *verschlüsselte* Passwort als Wert fest.

Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

# INFA\_NODE\_KEYSTORE\_PASSWORD

Die Umgebungsvariable INFA\_NODE\_KEYSTORE\_PASSWORD gilt für das infasetup-Befehlszeilenprogramm.

Einige *infasetup*-Befehle konfigurieren die sichere Kommunikation für die Domäne. Sie können das Passwort für die Informatica Java Keystore (JKS)-Datei als Option mit *infasetup* angeben, oder Sie können es als Umgebungsvariable INFA\_NODE\_KEYSTORE\_PASSWORD speichern.

Verwenden Sie die folgenden Schritte als Richtlinie zur Verwendung eines verschlüsselten Passworts als eine Umgebungsvariable:

1. Verwenden Sie das Befehlszeilenprogramm *pmpasswd* zum Verschlüsseln des Datenbankbenutzerpassworts.

*pmpasswd* generiert und zeigt das verschlüsselte Passwort an. Wenn Sie beispielsweise das Passwort „monday“ eingeben, wird dieses wie folgt verschlüsselt: f/wRb5PZsZnqESTDPeos7Q==.

2. Konfigurieren Sie die Passwortumgebungsvariable, um den verschlüsselten Wert festzulegen.

## Konfigurieren von INFA\_NODE\_KEYSTORE\_PASSWORD unter UNIX

So konfigurieren Sie INFA\_NODE\_KEYSTORE\_PASSWORD unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:

```
pmpasswd <database password>
```

*pmpasswd* gibt das verschlüsselte Passwort zurück.

2. Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv INFA_NODE_KEYSTORE_PASSWORD <encrypted password>
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
INFA_NODE_KEYSTORE_PASSWORD = <encrypted password>  
export INFA_NODE_KEYSTORE_PASSWORD
```

## Konfigurieren von INFA\_NODE\_KEYSTORE\_PASSWORD unter Windows

So konfigurieren Sie INFA\_NODE\_KEYSTORE\_PASSWORD unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:

```
pmpasswd <database password>
```

*pmpasswd* gibt das verschlüsselte Passwort zurück.

2. Geben Sie die Umgebungsvariable INFA\_NODE\_KEYSTORE\_PASSWORD ein und legen Sie das *verschlüsselte* Passwort als Wert fest.

Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

# INFA\_NODE\_TRUSTSTORE\_PASSWORD

Die Umgebungsvariable `INFA_NODE_TRUSTSTORE_PASSWORD` gilt für das `infasetup`-Befehlszeilenprogramm.

Einige `infasetup`-Befehle konfigurieren die sichere Kommunikation für die Domäne. Sie können das Passwort für die Datei `infa_truststore.jks` als Option mit `infasetup` angeben, oder Sie können es als Umgebungsvariable `INFA_NODE_TRUSTSTORE_PASSWORD` speichern.

Verwenden Sie die folgenden Schritte als Richtlinie zur Verwendung eines verschlüsselten Passworts als eine Umgebungsvariable:

1. Verwenden Sie das Befehlszeilenprogramm `pmpasswd` zum Verschlüsseln des Datenbankbenutzerpassworts.  
  
`pmpasswd` generiert und zeigt das verschlüsselte Passwort an. Wenn Sie beispielsweise das Passwort „monday“ eingeben, wird dieses wie folgt verschlüsselt: `f/wRb5PZsZnqESTDPeos7Q==`.
2. Konfigurieren Sie die Passwortumgebungsvariable, um den verschlüsselten Wert festzulegen.

## Konfigurieren von `INFA_NODE_TRUSTSTORE_PASSWORD` unter UNIX

So konfigurieren Sie `INFA_NODE_TRUSTSTORE_PASSWORD` unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:  

```
pmpasswd <database password>
```

  
`pmpasswd` gibt das verschlüsselte Passwort zurück.
2. Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:  

```
setenv INFA_NODE_TRUSTSTORE_PASSWORD <encrypted password>
```

  
Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:  

```
INFA_NODE_TRUSTSTORE_PASSWORD = <encrypted password>
export INFA_NODE_TRUSTSTORE_PASSWORD
```

## Konfigurieren von `INFA_NODE_TRUSTSTORE_PASSWORD` unter Windows

So konfigurieren Sie `INFA_NODE_TRUSTSTORE_PASSWORD` unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:  

```
pmpasswd <database password>
```

  
`pmpasswd` gibt das verschlüsselte Passwort zurück.
2. Geben Sie die Umgebungsvariable `INFA_NODE_TRUSTSTORE_PASSWORD` ein und legen Sie das verschlüsselte Passwort als Wert fest.  
  
Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

# INFA\_REPCNX\_INFO

Die `INFA_REPCNX_INFO`-Umgebungsvariable gilt für das `pmrep`-Befehlszeilenprogramm.

Wenn Sie *pmrep* im Befehlszeilenmodus oder über ein Skript ausführen, werden die Repository-Verbindungsinformationen in einer Datei namens *pmrep.cnx* gespeichert. *pmrep* verwendet die Informationen in dieser Datei für eine erneute Verbindung zum Repository. Die Umgebungsvariable *INFA\_REPCNX\_INFO* speichert den Dateinamen und Dateipfad für die Repository-Verbindungsdatei. Bei jeder Ausführung von *pmrep connect* löscht der Befehl die Datei „*pmrep.cnx*“. Wenn der *pmrep connect*-Befehl erfolgreich ausgeführt wird, wird die Datei „*pmrep.cnx*“ durch die Repository-Verbindungsinformationen ersetzt.

Verwenden Sie diese Variable, wenn Skripts, die *pmrep*-Befehle ausgeben, gleichzeitig ausgeführt werden und Verbindungen zu anderen Repositories herstellen. Geben Sie in jeder Shell eine andere Repository-Verbindungsdatei an. Dies verhindert, dass ein Skript die von einem anderen Skript verwendeten Verbindungsinformationen überschreibt.

Wenn Sie diese Umgebungsvariable nicht festlegen, speichert *pmrep* Verbindungsinformationen in der *pmrep.cnx*-Datei im Basisverzeichnis. Wenn Sie die Datei „*pmrep.cnx*“ für einen anderen Speicherort festlegen möchten, geben Sie den Dateipfad mit der Umgebungsvariable *INFA\_REPCNX\_INFO* an.

## Konfigurieren von *INFA\_REPCNX\_INFO* unter UNIX

So konfigurieren Sie *INFA\_REPCNX\_INFO* unter UNIX:

- Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv INFA_REPCNX_INFO <file name>
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
INFA_REPCNX_INFO = <file name>  
export INFA_REPCNX_INFO
```

## Konfigurieren von *INFA\_REPCNX\_INFO* unter Windows

So konfigurieren Sie *INFA\_REPCNX\_INFO* unter Windows:

- Geben Sie in einer DOS-Shell Folgendes ein:

```
set INFA_REPCNX_INFO = <file name>
```

**Hinweis:** Wenn Sie mehrere *pmrep*-Skripts ausführen, legen Sie diese Umgebungsvariable für die DOS-Shell fest, nicht für den Rechner.

# INFA\_REPOSITORY\_PASSWORD

Die *INFA\_REPOSITORY\_PASSWORD*- Umgebungsvariable gilt für das *infacmd*-Befehlszeilenprogramm.

Für einige *infacmd*-Befehle ist ein PowerCenter Repository-Passwort erforderlich. Sie können ein Benutzerpasswort als eine Option mit *infacmd* bereitstellen oder es als Umgebungsvariable *INFA\_REPOSITORY\_PASSWORD* speichern.

Verwenden Sie die folgenden Schritte als Richtlinie zur Verwendung eines verschlüsselten Passworts als eine Umgebungsvariable:

1. Verwenden Sie das Befehlszeilenprogramm *pmpasswd* zum Verschlüsseln des Benutzerpassworts. *pmpasswd* generiert und zeigt das verschlüsselte Passwort an. Wenn Sie beispielsweise das Passwort "monday" eingeben, wird dieses wie folgt verschlüsselt: f/wRb5PZsZnqESTDPeos7Q==.
2. Konfigurieren Sie die Passwortumgebungsvariable, um den verschlüsselten Wert festzulegen.

## VERWANDTE THEMEN:

- [“Encrypting Passwords” auf Seite 61](#)

## Konfigurieren von INFA\_REPOSITORY\_PASSWORD unter UNIX

So konfigurieren Sie INFA\_REPOSITORY\_PASSWORD unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:

```
pmpasswd <password>
```

*pmpasswd* gibt das verschlüsselte Passwort zurück.

2. Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv INFA_REPOSITORY_PASSWORD <encrypted password>
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
INFA_REPOSITORY_PASSWORD = <encrypted password>  
export INFA_REPOSITORY_PASSWORD
```

## Konfigurieren von INFA\_REPOSITORY\_PASSWORD unter Windows

So konfigurieren Sie INFA\_REPOSITORY\_PASSWORD unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:

```
pmpasswd <repository password>
```

*pmpasswd* gibt das verschlüsselte Passwort zurück.

2. Geben Sie die Umgebungsvariable INFA\_REPOSITORY\_PASSWORD ein und legen Sie das *verschlüsselte* Passwort als Wert fest.

Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

## INFATool\_DATEFORMAT

Die INFATool\_DATEFORMAT-Umgebungsvariable gilt für das pmcmd-Befehlszeilenprogramm.

Verwenden Sie diese Umgebungsvariable, um die Anzeige des Datums und der Uhrzeit unter Verwendung von *pmcmd* anzupassen. Geben Sie den Datumsformatstring im Format DY MON DD HH24:MI:SS YYYY ein. *pmcmd* überprüft, ob der String ein gültiges Format aufweist. Wenn der Formatstring ungültig ist, generiert der Integration Service eine Warnmeldung und zeigt das Datum im Format DY MON DD HH24:MI:SS YYYY an.

## Konfigurieren von INFATool\_DATEFORMAT unter UNIX

So konfigurieren Sie INFATool\_DATEFORMAT unter UNIX:

- Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv INFATool_DATEFORMAT <date/time format string>
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
INFATool_DATEFORMAT = <date/time format string>  
export INFATool_DATEFORMAT
```



## Konfigurieren von INFATool\_DATEFORMAT unter Windows

So konfigurieren Sie INFATool\_DATEFORMAT unter Windows:

- Geben Sie die Umgebungsvariable INFATool\_DATEFORMAT ein und legen Sie den Wert zum Anzeigen der Formatstring fest.

Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

## Encrypting Passwords

You can encrypt passwords to create an environment variable to use with infacmd, infasetup, pmcmd, and pmrep or to define a password in a parameter file.

For example, you can encrypt the repository and database passwords for pmrep to maintain security when using pmrep in scripts. Then you can create an environment variable to store the encrypted password. Or, you can define a password for a relational database connection object in a parameter file.

Use the command line program pmpasswd to encrypt passwords.

The pmpasswd utility uses a AES/CBC/PKCS5 padding cipher and generates a base64 encoded and AES 128-bit or AES 256-bit encrypted password.

The pmpasswd utility installs in the following directory:

```
<InformaticaInstallationDir>/server/bin
```

The pmpasswd utility uses the following syntax:

```
pmpasswd <password> [-e (CRYPT_DATA | CRYPT_SYSTEM)]
```

The following table describes pmpasswd options and arguments:

Option	Argument	Description
-	password	Required. The password to encrypt.
-e	CRYPT_DATA, CRYPT_SYSTEM	Optional. Encryption type: <ul style="list-style-type: none"><li>- CRYPT_DATA. Use to encrypt connection object passwords that you define in a parameter file.</li><li>- CRYPT_SYSTEM. Use for all other passwords.</li></ul> Default is CRYPT_SYSTEM.

By default, the pmpasswd utility generates AES 128-bit encrypted password. You can set the environment variable INFA\_USE\_AES\_256\_CRYPTOGRAPHER to *true* to enable AES 256-bit encryption for enhanced password security. In single node domain or multinode domain, ensure to shutdown the domain before setting or removing the environment variable.

When you enable the AES 256-bit encryption, the previously stored sensitive data in the environment variables does not work. You must encrypt such previously stored sensitive data again and reset the data in the environment variables after enabling AES 256-bit encryption. However, the license keys remain encrypted with AES 128-bit even if you enable AES 256-bit.

After you choose either AES 128-bit or AES 256-bit encryption, you must use the same encryption mechanism while performing a backup and restore or export and import operation. For example, if you back up a domain

or repository using the AES 128-bit mechanism, you must restore the domain or repository using the same 128-bit encryption mechanism. Domain restore fails if AES 256-bit encryption is enabled for domain backup and not enabled during domain restore. In such a case, clean up the database, enable 256-bit encryption and restore the domain again.

Similarly, if you export a domain or repository using the AES 128-bit mechanism, you must import the domain or repository using the same 128-bit encryption mechanism.

## Verwenden eines Passworts als eine Umgebungsvariable

Verwenden Sie die folgenden Schritte als Richtlinie zur Verwendung eines verschlüsselten Passworts als eine Umgebungsvariable:

1. Verwenden Sie das Befehlszeilenprogramm *pmpasswd* zum Verschlüsseln des Passworts.  
*pmpasswd* generiert und zeigt das verschlüsselte Passwort an. Wenn Sie beispielsweise das Passwort "monday" eingeben, wird das Passwort als "f/wRb5PZsZnqESTDPeos7Q==" verschlüsselt.
2. Konfigurieren Sie die Passwortumgebungsvariable, um den verschlüsselten Wert festzulegen.

## Konfigurieren eines Passworts als Umgebungsvariable unter UNIX

So konfigurieren Sie ein Passwort als Umgebungsvariable unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:  

```
pmpasswd <password>
```

  
*pmpasswd* gibt das verschlüsselte Passwort zurück.
2. Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:  

```
setenv <Password_Environment_Variable> <encrypted password>
```

  
Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:  

```
<Password_Environment_Variable> = <encrypted password>
export <Password_Environment_Variable>
```

  
Sie können der Umgebungsvariable jeden gültigen UNIX-Namen zuweisen.

## Konfigurieren eines Passworts als Umgebungsvariable unter Windows

So konfigurieren Sie ein Passwort als Umgebungsvariable unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:  

```
pmpasswd <password>
```

  
*pmpasswd* gibt das verschlüsselte Passwort zurück.
2. Geben Sie die Passwort-Umgebungsvariable im Variablenfeld ein. Geben Sie das Passwort *verschlüsselt* im Wertfeld ein.  
  
Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

# Festlegen des Benutzernamens

Für *pmcmd* und *pmrep* können Sie eine Umgebungsvariable zum Speichern des Benutzernamens erstellen.

## Konfigurieren eines Benutzernamens als eine Umgebungsvariable unter UNIX

So konfigurieren Sie einen Benutzernamen als eine Umgebungsvariable unter UNIX:

- Geben Sie in einer UNIX C-Shell-Umgebung Folgendes ein:

```
setenv <User_Name_Environment_Variable> <user name>
```

Geben Sie in einer UNIX Bourne-Shell-Umgebung Folgendes ein:

```
<User_Name_Environment_Variable> = <user name>  
export <User_Name_Environment_Variable>
```

Sie können der Umgebungsvariable jeden gültigen UNIX-Namen zuweisen.

## Konfigurieren eines Benutzernamens als eine Umgebungsvariable unter Windows

So konfigurieren Sie einen Benutzernamen als eine Umgebungsvariable unter Windows:

- Geben Sie die Benutzernamen-Umgebungsvariable im Variablen-Feld ein. Geben Sie den Benutzernamen im Wert-Feld ein.

Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

# KAPITEL 5

## Verwenden von infacmd

Dieses Kapitel umfasst die folgenden Themen:

- [Verwenden von infacmd - Übersicht, 64](#)
- [infacmd ListPlugins, 65](#)
- [Running Commands, 65](#)
- [Herstellen einer Verbindung zur Domäne, 66](#)
- [infacmd-Rückgabewerte, 67](#)

## Verwenden von infacmd - Übersicht

*infacmd* ist ein Befehlszeilenprogramm zum Verwalten von Domänen, Benutzern und Diensten. Verwenden Sie *infacmd*, um die folgenden Objekte und Dienste zu verwalten:

- **Anwendungsdienste und -prozesse.** Erstellen, aktivieren, deaktivieren und entfernen Sie den Status der Anwendungsdienste und der zugehörigen Dienstprozesse und rufen Sie diesen ab. Pingdienste. Listen Sie Dienste und die Knoten auf, auf denen sie ausgeführt werden. Aktualisieren Sie Dienstprozesse und Dienstprozessoptionen. Sie können mit *infacmd* keine Dienste einer früheren Version erstellen.
- **Domänen-Gateway.** Aktualisieren Sie die Verbindungsinformationen des Gateway-Knotens.
- **Domänen.** Verknüpfen Sie Domänen und entfernen Sie Domänenverknüpfungen. Ändern Sie das Passwort des Domänenadministrators. Aktualisieren Sie Domänenoptionen. Fügen Sie Dienstebenen hinzu und entfernen Sie diese.
- **Ordner.** Erstellen, verschieben, aktualisieren und entfernen Sie Ordner und listen Sie diese auf. Verschieben Sie Objekte zwischen Ordnern.
- **Gitter.** Erstellen und entfernen Sie Gitter. Listen Sie Knoten in einem Gitter auf.
- **Lizenzen.** Fügen Sie Lizenzen hinzu, entfernen Sie diese, listen Sie Lizenzen auf, weisen Sie Lizenzen zu und heben Sie die Zuweisung auf. Zeigen Sie Lizenzinformationen an.
- **Protokollereignisse.** Rufen Sie Protokollereignisse ab und bereinigen Sie diese. Rufen Sie Sitzungs- und Arbeitsablaufprotokolle ab. Wandeln Sie binäre Protokolldateien in Textdateien um.
- **Knoten.** Aktualisieren, pingen und entfernen Sie Knoten und fahren Sie diese herunter. Listen Sie Knotennamen und -optionen auf. Aktualisieren Sie die Knotenrolle. Fügen Sie Knotenressourcen hinzu, aktivieren, deaktivieren, entfernen Sie diese und listen Sie Knotenressourcen auf. Ändern Sie einen Knoten von einem Gateway-Knoten in einen Arbeitsknoten oder umgekehrt. Berechnen Sie das CPU-Profil für einen Knoten.

- **Benutzer.** Erstellen und entfernen Sie Benutzer. Setzen Sie Benutzerpasswörter zurück. Abonnieren Sie Alarmer für Benutzer und heben Sie Abonnements auf. Weisen Sie Benutzern Berechtigungen für Objekte zu. Aktivieren Sie die Benutzerkonten zum Sperren und Entsperren von Benutzerkonten.

## infacmd ListPlugins

Jedes infacmd-Programm hat eine Plugin-ID. Wenn Sie das Programm ausführen, nehmen Sie die Plugin-ID in den Programmnamen auf.

Dis fungiert beispielsweise als Plugin-ID für das infacmd-Programm des Data Integration Service.

Um beispielsweise einen Befehl auszuführen, der bereitgestellte Anwendungen auflistet, verwenden Sie den Befehl `infacmd dis ListApplications`:

```
infacmd dis ListApplications -dn domain_name -un user_name -d password -sn
Data_Integration_Service_Name
```

Geben Sie zum Auflisten der Plugin-IDs folgenden Befehl ein:

```
infacmd (.sh) ListPlugins
```

Geben Sie zum Auflisten der gültigen Befehle für ein Plugin folgenden Befehl ein:

```
infacmd(.sh) plugin_ID Help
```

Geben Sie zum Anzeigen von Hilfe zu einem Befehl folgenden Befehl ein:

```
infacmd(.sh) plugin_ID CommandName Help
```

## Running Commands

Invoke `infacmd` from the command line. You can issue commands directly or from a script, batch file, or other program.

To run `infacmd` commands:

1. At the command prompt, switch to the directory where the `infacmd` executable is located.  
By default, `infacmd` installs in the following directory of the Informatica services installation:  
<Informatica installation directory>/isp/bin
2. Enter `infacmd` on Windows or `infacmd.sh` on UNIX followed by the plugin ID, the command name, and the required options and arguments. The command names are not case sensitive.

For example:

```
infacmd(.sh) plugin_ID CommandName [-option1] argument_1 [-option2]
argument_2...Command Options
```

When you run `infacmd`, you enter options for each command, followed by the required arguments. For example, most commands require that you enter the domain name, user name, and password using command options. Command options are preceded with a hyphen and are not case sensitive. Arguments follow the option.

To enter an argument that is preceded with a hyphen, enclose the argument in quotation marks using the backslash (\) as an escape character before each quotation mark. For example, the following command

writes the log for the mapping run with the job ID "-qnLI7G\_TEEW9olHBkc9hoA" to the file "MyLog.log" within the infacmd directory on Windows:

```
infacmd ms GetRequestLog -dn MyDomain -sn MyDIS -un AdminUser -pd password -id \"-qnLI7G_TEEW9olHBkc9hoA\" -f MyLog.log
```

If you omit or incorrectly enter one of the required options, the command fails and infacmd returns an error message.

You can use environment variables for some command options with infacmd. For example, you can store the default user name and password for a domain as environment variables so that you do not have to enter them using command options. Configure these variables before you use infacmd.

## Herstellen einer Verbindung zur Domäne

Das infacmd-Befehlszeilenprogramm enthält Optionen, mit denen Sie eine Verbindung zur Domäne herstellen können. Diese Optionen können für alle Befehle verwendet werden.

In der folgenden Tabelle werden die infacmd-Optionen beschrieben, die für alle Befehle verwendet werden können:

Option	Beschreibung
-DomainName -dn	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt. Wenn die Domäne einen einzelnen Kerberos-Bereich für die Authentifizierung verwendet, geben Sie den SAM-Kontonamen für den Benutzer an. Wenn die Domäne die bereichsübergreifende Kerberos-Authentifizierung verwendet, geben Sie den Benutzerprinzipalnamen für den Benutzer an.
-Password -pd	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Beschreibung
-SecurityDomain -sdn	<p>Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Sie können einen Wert für -sdn angeben oder den Standardwert basierend auf dem Authentifizierungsmodus verwenden:</p> <ul style="list-style-type: none"> <li>- Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Zum Arbeiten mit der LDAP-Authentifizierung müssen Sie den Wert für -sdn angeben.</li> <li>- Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Wenn die Domäne die native Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</li> </ul> <p>Standardwert ist „Nativ“.</p>
-ResilienceTimeout -re	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## infacmd-Rückgabewerte

Das infacmd-Programm gibt die erfolgreiche oder fehlgeschlagene Ausführung eines Befehls mit den folgenden Rückgabewerten an:

- 0 gibt an, dass der Befehl erfolgreich ausgeführt wurde.
- -1 gibt an, dass der Befehl fehlgeschlagen ist.

Verwenden Sie den DOS- oder UNIX-echo-Befehl unmittelbar nach Ausführung eines infacmd-Befehls, um den Rückgabewert für den Befehl anzuzeigen:

- An einer DOS-Shell: `echo %ERRORLEVEL%`
- An einer UNIX Bourne- oder Korn-Shell: `echo $?`
- An einer UNIX C-Shell: `echo $status`

# KAPITEL 6

## infacmd as-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [CreateExceptionAuditTables, 68](#)
- [CreateService, 70](#)
- [DeleteExceptionAuditTables, 72](#)
- [ListServiceOptions, 73](#)
- [ListServiceProcessOptions, 73](#)
- [UpdateServiceOptions, 74](#)
- [UpdateServiceProcessOptions, 75](#)

### CreateExceptionAuditTables

Erstellt Tabellen, die Audit-Trail-Daten für die Arbeit enthalten können, die Benutzer des Analyst Tools in Ausnahmeverwaltungsaufgaben durchführen.

Der Befehl „infacmd as CreateExceptionAuditTables“ verwendet die folgende Syntax:

```
CreateExceptionAuditTables
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

**Hinweis:** Das infacmd-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter [“Herstellen einer Verbindung zur Domäne” auf Seite 66](#).



In der folgenden Tabelle werden die Optionen für den Befehl „infacmd as CreateExceptionAuditTables“ beschrieben:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-ServiceName -sn	Erforderlich. Name des Analyst-Diensts.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-ResilienceTimeout -re	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.

## Regeln und Richtlinien für Audit-Tabellen der Ausnahmeverwaltung

Bevor Sie Tabellen zum Speichern von Audit-Daten für Ausnahmeverwaltungsaufgaben erstellen, überprüfen Sie die folgenden Regeln und Richtlinien:

- Der Analyst-Dienst schreibt Audit-Daten für die Ausnahmeverwaltungsaufgaben, die von einem Datenintegrationsdienst bei der Ausführung eines Arbeitsablaufs erstellt werden, der eine Human-Aufgabe enthält. Jede Ausnahmeverwaltungsaufgabe stellt eine Instanz einer Human-Aufgabe in einem Arbeitsablauf dar.

Mit der Option „HumanTaskDataIntegrationService“ im Befehl „infacmd as createService help“ wird der Datenintegrationsdienst angegeben, der die Ausnahmeverwaltungsaufgaben erstellt.

- Bevor Sie die Audit-Tabellen der Ausnahmeverwaltung erstellen, geben Sie eine Datenbank und ein Schema für die Tabellen an. Führen Sie zur Angabe der Datenbank und des Schemas den Befehl „infacmd as updateServiceOptions“ aus.

Richten Sie bei Ausführung des Befehls „infacmd as updateServiceOptions“ folgende Optionen ein:

- o HumanTaskDataIntegrationService.exceptionDbName
- o HumanTaskDataIntegrationService.exceptionSchemaName

- Die Audit-Tabellen enthalten alle Audit-Trail-Daten für die Arbeit, die Benutzer in dem vom Analyst-Dienst angegebenen Analyst Tool durchführen. Wenn Sie die Audit-Tabellen nicht erstellen, übernimmt dies der Analyst-Dienst für jede Ausnahmeverwaltungsaufgabe in der Datenbank, die die Aufgabendaten enthält.

# CreateService

Erstellt einen Analyst-Dienst in einer Domäne. Verbindet darüber hinaus einen Modellrepository-, Datenintegrations- und Metadata Manager-Dienst mit dem Analyst-Dienst.

Der Befehl „infacmd as CreateService“ verwendet die folgende Syntax:

```
CreateService

<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-RepositoryService|-rs> model_repository_service_name]
[<-DataIntegrationService|-ds> data_integration_service_name]
[<-HumanTaskDataIntegrationService|-htds> human_task_data_integration_service_name]
[<-MetadataManagerService|-mm> metadata_manager_service_name]
[<-FlatFileCacheLocation|-ffl> flat_file_location]
[<-CatalogService|-cs> catalog_service_name]
[<-CatalogServiceUserName|-csau> catalog_service_user_name]
[<-CatalogServiceSecurityDomain|-cssdn> catalog_service_security_domain]
[<-CatalogServicePassword|-csap> catalog_service_password]
[<-RepositoryUsername|-au> model_repository_user_name]
[<-RepositorySecurityDomain|-rssdn> model_repository_security_domain]
[<-RepositoryPassword|-ap> model_repository_password]
[<-BusinessGlossaryExportFileDirectory|-bgefd> business_glossary_export_file_directory]
<-HttpPort> http_port
```

**Hinweis:** Das infacmd-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter [“Herstellen einer Verbindung zur Domäne“ auf Seite 66](#).

In der folgenden Tabelle werden die Optionen für den Befehl „infacmd as CreateService“ beschrieben:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-NodeName -nn	Erforderlich. Name des Knotens, auf dem der Analyst-Dienst ausgeführt wird.
-ServiceName -sn	Erforderlich. Name des Analyst-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositories kompatibel sein. Der Name darf maximal 230 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten:  / * ? < > "
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	Passwort für den Benutzernamen.

Option	Beschreibung
-SecurityDomain -sdn	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-ResilienceTimeout -re	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-RepositoryService -rs	Optional. Name des Modellrepository-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 230 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten:  / * ? < > "
-DataIntegrationService -ds	Optional. Der mit dem Analyst-Dienst verbundene Name des Datenintegrationsdiensts.
-HumanTaskDataIntegrationService -htds	Optional. Datenintegrationsdienst, der Arbeitsabläufe ausführt. Wenn ein Arbeitsablauf eine Human-Task enthält, melden sich Benutzer unter der URL des Analyst-Diensts an, um die Human-Task-Instanzen zu bearbeiten.
-MetadataManagerService -mm	Optional. Der mit dem Analyst-Dienst verbundene Name des Metadata Manager-Diensts.
-FlatFileCacheLocation -ffl	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, in dem die Einfachdateien zwischengespeichert werden sollen. Folgendes Format ist erforderlich: /<parent folder>/>child folder>
-CatalogService -cs	Optional. Name des Katalogdiensts, der dem Analyst-Dienst zugeordnet werden soll.
-CatalogServiceUserName -csau	Optional. Erforderlich, wenn Sie einen Katalogdienst angeben. Administratorbenutzername zum Herstellen einer Verbindung zum Katalogdienst.
-CatalogServiceSecurityDomain -cssdn	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Administrator-Benutzer gehört.
-CatalogServicePassword -csap	Erforderlich, wenn Sie einen Katalogdienst angeben. Benutzerpasswort für den Katalogdienst.
-RepositoryUserName -au	Erforderlich, wenn Sie einen Modellrepository-Dienst angeben. Benutzername für die Verbindung zum Modellrepository. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositorySecurityDomain -rssdn	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Administrator-Benutzer gehört.
-RepositoryPassword -ap	Erforderlich, wenn Sie einen Modellrepository-Dienst angeben. Benutzerpasswort für den Modellrepository-Dienst.

Option	Beschreibung
-BusinessGlossaryExportFileDirectory -bgefd	Optional. Speicherort des Verzeichnisses zum Exportieren von Geschäftsglossardateien.
-HttpPort	Erforderlich. Portnummer für den Analyst-Dienst.

## DeleteExceptionAuditTables

Löscht Tabellen, die Audit-Trail-Daten für die Arbeit enthalten können, die Benutzer des Analyst Tools in Ausnahmeverwaltungsaufgaben durchführen.

Der Befehl „infacmd as DeleteExceptionAuditTables“ verwendet die folgende Syntax:

```

DeleteExceptionAuditTables

<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]

```

**Hinweis:** Das infacmd-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter [„Herstellen einer Verbindung zur Domäne“ auf Seite 66](#).

In der folgenden Tabelle werden die Optionen für den Befehl „infacmd as DeleteExceptionAuditTables“ beschrieben:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-ServiceName -sn	Erforderlich. Name des Analyst-Diensts.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-ResilienceTimeout -re	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.

# ListServiceOptions

Listet Analyst-Dienst-Optionen auf. Listet die Werte für jede Analyst-Dienst-Option auf.

Der Befehl „infacmd as ListServiceOptions“ verwendet die folgende Syntax:

```
ListServiceOptions  
  
<-DomainName|-dn> domain_name  
<-ServiceName|-sn> service_name  
<-UserName|-un> user_name  
<-Password|-pd> password  
[<-SecurityDomain|-sdn> security_domain]  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

**Hinweis:** Das infacmd-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter [„Herstellen einer Verbindung zur Domäne“ auf Seite 66](#).

In der folgenden Tabelle werden die Optionen für den Befehl „infacmd as ListServiceOptions“ beschrieben:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-ServiceName -sn	Erforderlich. Name des Analyst-Diensts. Bei diesem Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-ResilienceTimeout -re	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.

# ListServiceProcessOptions

Listet die Analyst-Dienst-Prozessoptionen auf.

Der Befehl „infacmd as ListServiceProcessOptions“ verwendet die folgende Syntax:

```
ListServiceProcessOptions  
  
<-DomainName|-dn> domain_name  
<-ServiceName|-sn> service_name  
<-UserName|-un> user_name  
<-Password|-pd> password  
[<-SecurityDomain|-sdn> security_domain]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

**Hinweis:** Das infacmd-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter ["Herstellen einer Verbindung zur Domäne" auf Seite 66](#).

In der folgenden Tabelle werden die Optionen für den Befehl „infacmd as ListServiceProcessOptions“ beschrieben:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-ServiceName -sn	Erforderlich. Name des Analyst-Diensts. Bei diesem Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-ResilienceTimeout -re	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-NodeName -nn	Erforderlich. Knoten, auf dem der Analyst-Dienstprozess ausgeführt wird.

## UpdateServiceOptions

Aktualisiert Analyst-Dienstoptionen. Führen Sie zum Anzeigen der aktuellen Optionswerte infacmd as ListServiceOptions aus.

Der Befehl „infacmd as UpdateServiceOptions“ verwendet die folgende Syntax:

```
UpdateServiceOptions

<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-Options |-o> options]
```

**Hinweis:** Das infacmd-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die

Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter ["Herstellen einer Verbindung zur Domäne" auf Seite 66](#).

In der folgenden Tabelle werden die Optionen für den Befehl „infacmd as UpdateServiceOptions“ beschrieben:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-ServiceName -sn	Erforderlich. Name des Analyst-Diensts. Bei diesem Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-ResilienceTimeout -re	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-Options -o	Optional. Liste der zu konfigurierenden Optionen. Trennen Sie die einzelnen Optionen mit einem Leerzeichen. Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein. Beispiel:  ... -o option_name=value option_name="value 2" ...  Führen Sie zum Anzeigen der Optionen den infacmd as ListServiceOptions-Befehl aus.

## UpdateServiceProcessOptions

Aktualisiert Optionen für den Analyst-Dienst-Prozess. Führen Sie zum Anzeigen der Optionen den infacmd as ListServiceProcessOptions-Befehl aus.

Der Befehl „infacmd as UpdateServiceProcessOptions“ verwendet die folgende Syntax:

```
UpdateServiceProcessOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
<-Options|-o> options
```

**Hinweis:** Das infacmd-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter ["Herstellen einer Verbindung zur Domäne" auf Seite 66](#).

In der folgenden Tabelle werden die Optionen für den Befehl „infacmd as UpdateServiceProcessOptions“ beschrieben:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-ServiceName -sn	Erforderlich. Name des Analyst-Diensts.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-ResilienceTimeout -re	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-NodeName -nn	Erforderlich. Knoten, auf dem der Analyst-Dienstprozess ausgeführt wird.
-Options -o	<p>Erforderlich. Liste der zu konfigurierenden Optionen. Trennen Sie die einzelnen Optionen mit einem Leerzeichen. Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein. Beispiel:</p> <pre>... -o option_name=value option_name="value 2" ...</pre> <p>Führen Sie zum Anzeigen der Optionen den infacmd as ListServiceProcessOptions-Befehl aus.</p>



# KAPITEL 7

## infacmd aud-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [getDomainObjectPermissions, 77](#)
- [getPrivilegeAssociation, 78](#)
- [getUserGroupAssociation, 80](#)
- [getUserGroupAssociationForRoles, 81](#)
- [getUsersPersonalInfo, 82](#)

### getDomainObjectPermissions

Ruft die Liste der Domänenobjekte ab, für die die angegebenen Benutzer oder Gruppen Berechtigungen haben. Sie können Berichte für die angegebenen Benutzer oder Gruppen generieren.

Benutzer mit der Administratorrolle können diesen Befehl ausführen.

Der Befehl „infacmd aud getDomainObjectPermissions“ verwendet folgende Syntax:

```
getDomainObjectPermissions

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<<-ExistingUserNames|-eu> existing_user_names|
<-ExistingGroupNames|-eg> existing_group_names>
[<-ExistingSecurityDomain|-esd> existing_security_domain]
[<-Format|-fm> format_TEXT_CSV]
[<-OutputFile|-lo> output_file_name]
```

**Hinweis:** Das infacmd-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter [“Herstellen einer Verbindung zur Domäne” auf Seite 66](#).

Die folgende Tabelle beschreibt die Optionen und Argumente für „infacmd aud getDomainObjectPermissions“:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	Name der Sicherheitsdomäne, die Sie erstellen möchten und zu der der Domänenbenutzer gehört.
-Gateway -hp	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Geben Sie die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne an.
-ResilienceTimeout -re	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-ExistingUserNames -eu	Erforderlich, wenn Sie -ExistingGroupNames (-eg) nicht verwenden. Name des Benutzers oder einer Liste von Benutzern zum Ausführen der Berichte. Bei mehreren Benutzern trennen Sie jeden Benutzer durch ein Komma in der Befehlszeile.
-ExistingGroupNames -eg	Erforderlich, wenn Sie -ExistingUserName (-eu) nicht verwenden. Name der Gruppe oder einer Liste mit Gruppen zum Ausführen der Berichte. Bei mehreren Benutzern trennen Sie jede Gruppe durch ein Komma in der Befehlszeile.
-ExistingSecurityDomain -esd	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Sicherheitsdomäne, zu der der Benutzer oder die Gruppe gehört. Der Standardwert ist „Nativ“.
-Format -fm	Optional. Format der Ausgabedatei. Gültige Typen umfassen: - Text - CSV  Wenn Sie kein Format angeben, verwendet infacmd Textformat mit einer Zeilenlänge von 80 Zeichen.
-OutputFile -lo	Optional. Name und Dateipfad für die Ausgabedatei.  Wenn Sie keinen Ausgabedateinamen angeben, zeigt infacmd die Protokollereignisse auf dem Bildschirm an.

## getPrivilegeAssociation

Ruft Berechtigungen ab, die den Benutzern oder Gruppen zugewiesen wurden. Sie können die Benutzer oder Gruppen auswählen, für die Sie den Bericht generieren möchten.

Benutzer mit der Administratorrolle können diesen Befehl ausführen.

Der Befehl „infacmd aud getPrivilegeAssociation“ verwendet folgende Syntax:

```
getPrivilegeAssociation

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<<-ExistingUserNames|-eu> existing_user_names|
<-ExistingGroupNames|-eg> existing_group_names>
[<-ExistingSecurityDomain|-esd> existing_security_domain]
[<-Format|-fm> format_TEXT_CSV]
[<-OutputFile|-lo> output_file_name]
```

**Hinweis:** Das infacmd-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter [„Herstellen einer Verbindung zur Domäne“ auf Seite 66](#).

Die folgende Tabelle beschreibt die Optionen und Argumente für „infacmd aud getPrivilegeAssociation“:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-ExistingUserNames -eu	Erforderlich, wenn Sie -ExistingGroupNames (-eg) nicht verwenden. Name des Benutzers oder einer Liste von Benutzern zum Ausführen der Berichte. Bei mehreren Benutzern trennen Sie jeden Benutzer durch ein Komma in der Befehlszeile.
-ExistingGroupNames -eg	Erforderlich, wenn Sie -ExistingUserName (-eu) nicht verwenden. Name der Gruppe oder einer Liste mit Gruppen zum Ausführen der Berichte. Bei mehreren Benutzern trennen Sie jede Gruppe durch ein Komma in der Befehlszeile.
-ExistingSecurityDomain -esd	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Sicherheitsdomäne, zu der der Benutzer oder die Gruppe gehört. Der Standardwert ist „Nativ“.

Option	Beschreibung
-Format -fm	Optional. Format der Ausgabedatei. Gültige Typen umfassen: - Text - CSV  Wenn Sie kein Format angeben, verwendet infacmd Textformat mit einer Zeilenlänge von 80 Zeichen.
-OutputFile -lo	Optional. Name und Dateipfad für die Ausgabedatei.  Wenn Sie keinen Ausgabedateinamen angeben, zeigt infacmd die Protokollereignisse auf dem Bildschirm an.

## getUserGroupAssociation

Ruft eine Liste mit Benutzern ab, die zur Gruppe gehören, oder eine Liste mit Gruppen, die den angegebenen Benutzern zugewiesen wurden. Sie können die Benutzer oder Gruppen auswählen, für die Sie den Bericht generieren möchten.

Benutzer mit der Administratorrolle können diesen Befehl ausführen.

Der Befehl „infacmd aud getUserGroupAssociation“ verwendet folgende Syntax:

```
getUserGroupAssociation

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<<-ExistingUserNames|-eu> existing_user_names|
<-ExistingGroupNames|-eg> existing_group_names>
[<-ExistingSecurityDomain|-esd> existing_security_domain]
[<-Format|-fm> format_TEXT_CSV]
[<-OutputFile|-lo> output_file_name]
```

**Hinweis:** Das infacmd-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter [“Herstellen einer Verbindung zur Domäne” auf Seite 66](#).

Die folgende Tabelle beschreibt die Optionen und Argumente für „infacmd aud getUserGroupAssociation“:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	Das Passwort für den Benutzernamen.

Option	Beschreibung
-SecurityDomain -sdn	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-ExistingUserNames -eu	Erforderlich, wenn Sie -ExistingGroupNames (-eg) nicht verwenden. Name des Benutzers oder einer Liste von Benutzern zum Ausführen der Berichte. Bei mehreren Benutzern trennen Sie jeden Benutzer durch ein Komma in der Befehlszeile.
-ExistingGroupNames -eg	Erforderlich, wenn Sie -ExistingUserName (-eu) nicht verwenden. Name der Gruppe oder einer Liste mit Gruppen zum Ausführen der Berichte. Bei mehreren Benutzern trennen Sie jede Gruppe durch ein Komma in der Befehlszeile.
-ExistingSecurityDomain -esd	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Sicherheitsdomäne, zu der der Benutzer oder die Gruppe gehört. Der Standardwert ist „Nativ“.
-Format -fm	Optional. Format der Ausgabedatei. Gültige Typen umfassen: - Text - CSV  Wenn Sie kein Format angeben, verwendet infacmd Textformat mit einer Zeilenlänge von 80 Zeichen.
-OutputFile -lo	Optional. Name und Dateipfad für die Ausgabedatei.  Wenn Sie keinen Ausgabedateinamen angeben, zeigt infacmd die Protokollereignisse auf dem Bildschirm an.

## getUserGroupAssociationForRoles

Ruft eine Liste mit Rollen ab, die Benutzern und Gruppen zugewiesen sind. Sie können die Rollen auswählen, für die Sie den Bericht generieren möchten.

Benutzer mit der Administratorrolle können diesen Befehl ausführen.

Der Befehl „infacmd aud getUserGroupAssociationForRoles“ verwendet folgende Syntax:

```

getUserGroupAssociationForRoles

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-RoleNames|-en> role_names
[<-Format|-fm> format_TEXT_CSV]
[<-OutputFile|-lo> output_file_name]
```

**Hinweis:** Das infacmd-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die

Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter ["Herstellen einer Verbindung zur Domäne" auf Seite 66](#).

Die folgende Tabelle beschreibt die Optionen und Argumente für „infacmd aud getUserGroupAssociationForRoles“:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-RoleNames -en	Erforderlich. Name der zugewiesenen Rolle für Benutzer oder Gruppen in der Domäne, für die Sie den Bericht generieren möchten. Bei mehreren Rollen trennen Sie jede Rolle durch ein Komma in der Befehlszeile.
-Format -fm	Optional. Format der Ausgabedatei. Gültige Typen umfassen: - Text - CSV  Wenn Sie kein Format angeben, verwendet infacmd Textformat mit einer Zeilenlänge von 80 Zeichen.
-OutputFile -lo	Optional. Name und Dateipfad für die Ausgabedatei.  Wenn Sie keinen Ausgabedateinamen angeben, zeigt infacmd die Protokollereignisse auf dem Bildschirm an.

## getUsersPersonalInfo

Ruft Benutzerinformationen in der Domäne ab. Der Bericht zeigt den vollständigen Namen, die Sicherheitsdomäne, die Beschreibung, die Kontaktdetails und den Benutzerstatus an. Wenn Sie den Bericht für Benutzer ausführen, zeigt der Bericht die Benutzerinformationen für die angegebenen Benutzer. Wenn Sie den Bericht für Gruppen ausführen, organisiert der Bericht Benutzerinformationen für alle Benutzer in der angegebenen Gruppe. Der Bericht zeigt die geschachtelten Gruppen separat an.

Benutzer mit der Administratorrolle können diesen Befehl ausführen.

Der Befehl „infacmd aud getUsersPersonalInfo“ verwendet folgende Syntax:

```
getUsersPersonalInfo

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<<-ExistingUserNames|-eu> existing_user_names|
<-ExistingGroupNames|-eg> existing_group_names>
[<-ExistingSecurityDomain|-esd> existing_security_domain]
[<-Format|-fm> format_TEXT_CSV]
[<-OutputFile|-lo> output_file_name]
```

**Hinweis:** Das infacmd-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter [„Herstellen einer Verbindung zur Domäne“ auf Seite 66](#).

Die folgende Tabelle beschreibt die Optionen und Argumente für „infacmd aud getUsersPersonalInfo“:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen
-ExistingUserNames -eu	Erforderlich, wenn Sie -ExistingGroupNames (-eg) nicht verwenden. Name des Benutzers oder einer Liste von Benutzern zum Ausführen der Berichte. Bei mehreren Benutzern trennen Sie jeden Benutzer durch ein Komma in der Befehlszeile.
-ExistingGroupNames -eg	Erforderlich, wenn Sie -ExistingUserName (-eu) nicht verwenden. Name der Gruppe oder einer Liste mit Gruppen zum Ausführen der Berichte. Bei mehreren Benutzern trennen Sie jede Gruppe durch ein Komma in der Befehlszeile.
-ExistingSecurityDomain -esd	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Sicherheitsdomäne, zu der der Benutzer oder die Gruppe gehört. Der Standardwert ist „Nativ“.

Option	Beschreibung
-Format -fm	Optional. Format der Ausgabedatei. Gültige Typen umfassen: - Text - CSV Wenn Sie kein Format angeben, verwendet infacmd Textformat mit einer Zeilenlänge von 80 Zeichen.
-OutputFile -lo	Optional. Name und Dateipfad für die Ausgabedatei. Wenn Sie keinen Ausgabedateinamen angeben, zeigt infacmd die Protokollereignisse auf dem Bildschirm an.



## KAPITEL 8

# infacmd autotune-Befehlsreferenz

- [Autotune, 85](#)

## Autotune

Konfiguriert Dienste und Verbindungen mit empfohlenen Einstellungen auf Grundlage des Bereitstellungstyps. Änderungen werden nach dem Neustart der Dienste wirksam.

Für jeden angegebenen Dienst werden die Änderungen am Dienst auf allen Knoten wirksam, die derzeit für die Ausführung des Diensts konfiguriert sind, und die Änderungen wirken sich auf alle Dienstprozesse aus.

Der Befehl `infacmd autotune` verwendet die folgende Syntax:

`Autotune`

```
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Size|-s> tuning_size_name
[<-ServiceNames|-sn> service_names]
[<-BlazeConnectionNames|-bcn> connection_names]
[<-SparkConnectionNames|-scn> connection_names]
[<-All|-a> yes_or_no]
```

Das `infacmd`-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die Tabelle mit den Optionen enthält Kurzbeschreibungen. Weitere Informationen zum Herstellen einer Verbindung zur Domäne finden Sie in der Befehlsreferenz.

In der folgenden Tabelle werden die Optionen und Argumente für `infacmd Autotune` beschrieben:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	Das Passwort für den Benutzernamen.

Option	Beschreibung
-SecurityDomain -sdn	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-ResilienceTimeout -re	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-Size -s	Erforderlich. Der Bereitstellungstyp, der hohe Datenverarbeitungsanforderungen auf der Grundlage von Parallelität und Volumen darstellt. Sie können Sandbox, Basic, Standard oder Advanced eingeben.
-ServiceNames -sn	Optional. Liste der Dienste, die in der Informatica-Domäne konfiguriert sind. Trennen Sie die einzelnen Dienstnamen durch ein Komma. Sie können die folgenden Dienste optimieren: <ul style="list-style-type: none"> <li>- Analyst-Dienst</li> <li>- Content-Management-Dienst</li> <li>- Datenintegrationsdienst</li> <li>- Modellrepository-Dienst</li> <li>- Ressourcenmanager-Dienst</li> <li>- Suchdienst</li> </ul> Standardwert ist „Keine“.
-BlazeConnectionNames -bcn	Optional. Liste der Hadoop-Verbindungen, die in der Informatica-Domäne konfiguriert sind. Für jede Hadoop-Verbindung optimiert der Befehl die Blaze-Konfigurationseigenschaften in der Hadoop-Verbindung. Trennen Sie die einzelnen Hadoop-Verbindungsnamen durch ein Komma. Standardwert ist „Keine“.
-SparkConnectionNames -scn	Optional. Liste der Hadoop-Verbindungen, die in der Informatica-Domäne konfiguriert sind. Für jede Hadoop-Verbindung optimiert der Befehl die Spark-Konfigurationseigenschaften in der Hadoop-Verbindung. Trennen Sie die einzelnen Hadoop-Verbindungsnamen durch ein Komma. Standardwert ist „Keine“.
-All -a	Optional. Geben Sie <code>yes</code> ein, um die empfohlenen Einstellungen für alle Analyst-Dienste, Content-Management-Dienste, Datenintegrationsdienste, Modellrepository-Dienste, Ressourcen-Manager-Dienste, Suchdienste und Hadoop-Verbindungen in der Informatica-Domäne anzuwenden. Geben Sie <code>no</code> ein, um die empfohlenen Einstellungen nur auf die von Ihnen angegebenen Dienste und Hadoop-Verbindungen anzuwenden. Standardwert ist <code>no</code> .

# KAPITEL 9

## Infacmd bg-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [upgradeRepository, 87](#)
- [deleteAuditHisotry, 88](#)
- [listGlossary, 89](#)
- [exportGlossary, 90](#)
- [importGlossary, 92](#)

### upgradeRepository

Aktualisiert die Unternehmensglossardaten im Modellrepository. Führen Sie diesen Befehl aus, nachdem Sie die Domäne und den Modellrepository-Dienst aktualisiert haben.

Der infacmd bg upgradeRepository-Befehl verwendet die folgende Syntax:

```
upgradeRepository

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-AtServiceName|-atn> Analyst_service_name
```

**Hinweis:** Das infacmd-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter ["Herstellen einer Verbindung zur Domäne" auf Seite 66](#).

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd bg upgradeRepository“ beschrieben:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne.

Option	Beschreibung
-Password -pd	Password für den Benutzernamen.
-SecurityDomain -sdn	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
AtServiceName -atn	Erforderlich. Name des Analyst-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 230 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten:  / * ? < > "

## deleteAuditHisotry

Löscht den Audit-Verlauf eines Glossars aus dem Analyst Tool.

Der Befehl „infacmd bg deleteAuditHistory“ verwendet die folgende Syntax:

```
deleteAuditHistory
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-AtServiceName|-atn> Analyst_service_name
<-GlossaryIdentity|-gi> Glossary_Identity
```

**Hinweis:** Das infacmd-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter [“Herstellen einer Verbindung zur Domäne” auf Seite 66](#).

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd bg deleteAuditHistory“ beschrieben:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	Password für den Benutzernamen.

Option	Beschreibung
-SecurityDomain -sdn	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
AtServiceName -atn	Erforderlich. Name des Analyst-Diensts.  Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 230 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten:  / * ? < > "
-GlossaryIdentity -gl	Erforderlich. Die Identität des Glossars, für das der Audit-Verlauf gelöscht werden soll. Sie können die Identität des Glossars mithilfe der Option <code>select PSB_EXTERNID from PO_BGGLOSSARY where POB_NAME = '&lt;glossary_name&gt;'</code> aus der Datenbank des Modellrepository-Diensts abrufen.

## listGlossary

Zeigt eine Liste der im Analyst Tool als Standardausgabe verfügbaren Unternehmensglossare an. Jeder Glossarname wird als separate Zeile angezeigt.

Der Befehl „`infacmd bg listGlossary`“ verwendet die folgende Syntax:

```
listGlossary

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-AtServiceName|-atn> Analyst_service_name
```

**Hinweis:** Das `infacmd`-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter [“Herstellen einer Verbindung zur Domäne” auf Seite 66](#).

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd bg upgradeRepository`“ beschrieben:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-UserName -un	Der Name der Informatica-Domäne.
-Password -pd	Passwort für den Benutzernamen.

Option	Beschreibung
-SecurityDomain -sdn	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
AtServiceName -atn	Erforderlich. Name des Analyst-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositories kompatibel sein. Der Name darf maximal 230 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten:  / * ? < > "

## exportGlossary

Exportiert die im Analyst Tool verfügbaren Unternehmensglossare. Das Analyst Tool exportiert Unternehmensglossardaten im XLSX- oder ZIP-Format, basierend auf den von Ihnen angegebenen Optionen.

Der Befehl „infacmd bg exportGlossary“ verwendet die folgende Syntax:

```
exportGlossary

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-AtServiceName|-atn> Analyst_service_name
[<-GlossaryList|-gl> Glossary_list]
[<-Delimiter|-dl> Glossary_name_delimiter]
[<-IncludeCrossGlossaryLinks|-cgl> Include_cross_glossary_links_true_false]
[<-IncludeAuditHistory|-ah> Include_audit_history_true_false]
[<-IncludeAttachment|-att> Include_attachments_true_false]
[<-IncludeOnlyTemplate|-tem> Include_templates_only_true_false]
[<-ExportasPlainTextOnly|-ept> Export_richtext_as_plain_text_true_false]
[<-status|-s> Status_of_assets]
[<-phase|-p> Phase_of_assets]
<-ExportFilePath|-ep> Export_path
```

**Hinweis:** Das infacmd-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter [“Herstellen einer Verbindung zur Domäne” auf Seite 66](#).

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd bg exportGlossary“ beschrieben:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne.

Option	Beschreibung
-Password -pd	Password für den Benutzernamen.
-SecurityDomain -sdn	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
AtServiceName -atn	Erforderlich. Name des Analyst-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 230 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten:  / * ? < > "
-GlossaryList -gl	Optional. Die Namen von einem oder mehreren Glossaren, die Sie exportieren möchten und auf die Sie gemäß der im Analyst Tool festgelegten Berechtigungen Zugriff haben. Trennen Sie bei mehreren Glossaren die Namen durch das benutzerdefinierte Delimiter-Zeichen.  Wenn Sie die Namen der Glossare nicht angeben, exportiert das Analyst Tool alle Glossare, auf die Sie gemäß der im Analyst Tool festgelegten Berechtigungen Zugriff haben.
-Delimiter -dl	Optional. Geben Sie einen benutzerdefinierten Delimiter an, wenn Sie mehrere Glossare exportieren und eines davon das Standard-Delimiter-Zeichen im Glossarnamen enthält. Der Standard-Delimiter ist ein Komma.  Definieren Sie einen benutzerdefinierten Delimiter mit maximal einem Sonderzeichen. Verwenden Sie den benutzerdefinierten Delimiter zum Trennen der Namen von mehreren Glossaren.
-IncludeCrossGlossaryLinks -cgl	Optional. Geben Sie einen der folgenden Werte ein: - True, um Querverweise des Glossars in die Exportdatei einzuschließen. - False, um Querverweise des Glossars in der Exportdatei zu überspringen. Standardwert ist „true“.
-IncludeAuditHistory -ah	Optional. Geben Sie einen der folgenden Werte ein: - True, um die Audit-Trail-Historie in die Exportdatei einzuschließen. - False, um die Audit-Trail-Historie in der Exportdatei zu überspringen. Standardwert ist „False“. <b>Hinweis:</b> Wenn Sie die Option "Audit-Verlauf einschließen (-ah)" auf "true" festlegen, werden die Business Glossary-Daten im ZIP-Format exportiert.
-IncludeAttachments -att	Optional. Geben Sie einen der folgenden Werte ein: - True, um Anhänge in die Exportdatei einzuschließen. - Geben Sie False an, um Anhänge in der Exportdatei zu überspringen. Standardwert ist „False“. <b>Hinweis:</b> Wenn Sie die Option "Anhänge einschließen (-att)" auf "true" festlegen, werden die Business Glossary-Daten im ZIP-Format exportiert.
-IncludeOnlyTemplates -tem	Optional. Geben Sie einen der folgenden Werte ein: - True, um nur Vorlagen in die Exportdatei einzuschließen. - False, um sowohl Vorlagen als auch Glossardaten in die Exportdatei einzuschließen. Standardwert ist „False“.

Option	Beschreibung
-ExportasPlainTextOnly -ept	Optional. Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- True, um formatierten Rich-Text-Inhalt als Klartext zu exportieren.</li> <li>- False, um formatierten Rich-Text-Inhalt als Rich-Text zu exportieren.</li> </ul> Standardwert ist „False“.
-status -s	Optional. Geben Sie einen oder alle der folgenden Werte durch ein Komma abgetrennt ein: <ul style="list-style-type: none"> <li>- Active, um Objekte zu exportieren, die aktiv sind.</li> <li>- Inactive, um Objekte zu exportieren, die inaktiv sind.</li> </ul> Das Analyst Tool exportiert Objekte, die sowohl aktiv als auch inaktiv sind, wenn Sie keinen Wert angeben.
-phase -p	Optional. Geben Sie einen oder alle der folgenden Werte durch ein Komma abgetrennt ein: <ul style="list-style-type: none"> <li>- Draft, um Objekte zu exportieren, die sich in der Phase „Entwurf“ befinden.</li> <li>- In_Review, um Objekte zu exportieren, die sich in der Phase „Überprüfung“ befinden.</li> <li>- Published, um Objekte zu exportieren, die sich in der Phase „Veröffentlicht“ befinden.</li> <li>- Rejected, um Objekte zu exportieren, die sich in der Phase „Abgelehnt“ befinden.</li> <li>- Pending_publish, um Objekte zu exportieren, die sich in der Phase „Zur Veröffentlichung ausstehend“ befinden.</li> </ul> Das Analyst Tool exportiert Objekte, die sich in allen Phasen befinden, wenn Sie keinen Wert angeben.
-ExportFilePath -ep	Erforderlich. Geben Sie den Pfad an, in dem das Befehlszeilenprogramm die exportierten Dateien speichern muss.

## importGlossary

Importiert Unternehmensglossare aus XLSX- oder ZIP-Dateien, die aus dem Analyst Tool exportiert wurden.

Der Befehl „infacmd bg importGlossary“ verwendet die folgende Syntax:

```
importGlossary

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-AtServiceName|-atn> Analyst_service_name
[<-GlossaryList|-gl> Glossary_list]
[<-Delimiter|-dl> Glossary_name_delimiter]
[<-IncludeCrossGlossaryLinks|-cgl> Include_cross_glossary_links_true_false]
[<-IncludeAuditHistory|-ah> Include_audit_history_true_false]
[<-IncludeAttachment|-att> Include_attachments_true_false]
[<-IncludeOnlyTemplate|-tem> Include_templates_only_true_false]
[<-IncludeRichTextContentforConflictingAssets|-irt>
Include_richtextcontent_conflicting_assets_true_false]
<-ImportFilePath|-ip> Import_path
[<-ResolutionOnMatchByName|-rmn> Copy_or_replace_or_skip_assets_by_name]
[<-ResolutionOnMatchById|-rmi> Copy_or_replace_or_skip_assets_by_id]
```



**Hinweis:** Das infacmd-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter ["Herstellen einer Verbindung zur Domäne" auf Seite 66](#).

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd bg importGlossary“ beschrieben:

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	Passwort für den Benutzernamen.
-SecurityDomain -sdn	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
AtServiceName -atn	Erforderlich. Name des Analyst-Diensts.  Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 230 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten:  / * ? < > "
GlossaryList -gl	Optional. Die Namen von einem oder mehreren Glossaren, die Sie importieren möchten und auf die Sie gemäß der im Analyst Tool festgelegten Berechtigungen Zugriff haben. Die Glossare müssen sich in der XLSX-Datei befinden. Trennen Sie bei mehreren Glossaren die Namen durch das benutzerdefinierte Delimiter-Zeichen.  Wenn Sie die Namen der Glossare nicht angeben, importiert das Analyst Tool alle Glossare, auf die Sie gemäß der im Analyst Tool festgelegten Berechtigungen Zugriff haben.
-Delimiter -dl	Optional. Geben Sie einen benutzerdefinierten Delimiter an, wenn Sie mehrere Glossare importieren und eines davon das Standard-Delimiter-Zeichen im Glossarnamen enthält. Der Standard-Delimiter ist ein Komma.  Definieren Sie einen benutzerdefinierten Delimiter mit maximal einem Sonderzeichen. Verwenden Sie den benutzerdefinierten Delimiter zum Trennen der Namen von mehreren Glossaren.
IncludeCrossGlossaryLinks -cgl	Optional. Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- <code>True</code>, um Querverweise des Glossars aus der Exportdatei zu importieren.</li> <li>- <code>False</code>, um das Importieren von Querverweisen des Glossars aus der Exportdatei zu überspringen.</li> </ul> Standardwert ist „true“.

Option	Beschreibung
-IncludeAuditHistory -ah	Optional. Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- <b>True</b>, um die Audit-Trail-Historie aus der Exportdatei zu importieren.</li> <li>- <b>False</b>, um das Importieren der Audit-Trail-Historie aus der Exportdatei zu überspringen.</li> </ul> Standardwert ist „False“.
-IncludeAttachments -att	Optional. Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- <b>True</b>, um beim Importieren von Unternehmensglossaren Anhänge einzuschließen.</li> <li>- <b>False</b>, um beim Importieren von Unternehmensglossaren sowohl Vorlagen als auch Glossardaten einzuschließen.</li> </ul> Standardwert ist „true“.
-IncludeOnlyTemplates -tem	Erforderlich. Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- <b>True</b>, um beim Importieren von Unternehmensglossaren nur Vorlagen einzuschließen.</li> <li>- <b>False</b>, um beim Importieren von Unternehmensglossaren sowohl Vorlagen als auch Glossardaten einzuschließen.</li> </ul> Standardwert ist „False“.
-IncludeRichTextContentforConflictingAssets -irt	Optional. Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- <b>True</b>, wenn Sie Rich-Text-Inhalt für kollidierende Objekte importieren möchten.</li> <li>- <b>False</b>, wenn Sie keinen Rich-Text-Inhalt für kollidierende Objekte importieren möchten.</li> </ul> Standardwert ist „True“.
-ImportFilePath -ip	Erforderlich. Geben Sie den Pfad, in dem die Importdatei verfügbar ist, und den Dateinamen an.
-ResolutionOnMatchByName -rmn	Optional. Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- <b>Copy</b>, um alle Objekte zu kopieren, wenn ein auf dem Namen basierender Konflikt vorhanden ist.</li> <li>- <b>Replace</b>, um alle Objekte zu ersetzen, wenn ein auf dem Namen basierender Konflikt vorhanden ist. Dies ist der Standardwert.</li> <li>- <b>Skip</b>, um alle Objekte zu überspringen, wenn ein auf dem Namen basierender Konflikt vorhanden ist.</li> </ul>
-ResolutionOnMatchById -rmi	Optional. Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- <b>Copy</b>, um alle Objekte zu kopieren, wenn ein auf der Objekt-ID basierender Konflikt vorhanden ist.</li> <li>- <b>Replace</b>, um alle Objekte zu ersetzen, wenn ein auf der Objekt-ID basierender Konflikt vorhanden ist. Dies ist der Standardwert.</li> <li>- <b>Skip</b>, um alle Objekte zu überspringen, wenn ein auf der Objekt-ID basierender Konflikt vorhanden ist.</li> </ul>

# KAPITEL 10

## infacmd ccps-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [deleteClusters, 95](#)
- [listClusters, 97](#)
- [updateADLSCertificate, 99](#)

### deleteClusters

Löscht vom Cluster-Arbeitsablauf erstellte Cluster aus der Cloud-Plattform.

Der Befehl „infacmd ccps deleteClusters“ verwendet die folgende Syntax:

```
deleteClusters
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
<-CloudProvisioningConfigurationID|-cpcid> cloud_provisioning_configuration_id
<-ClusterIDs|-cids> cluster_ids
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

**Hinweis:** Wenn Sie diesen Befehl zum Löschen von Clustern auf der Cloud-Plattform Azure verwenden, blockiert der Prozess jeden anderen Befehl über die Befehlsshell, bis Azure den Prozess zum Freigeben von Clusterressourcen abgeschlossen hat. Dieser Vorgang kann mehrere Minuten dauern. Wenn Sie versuchen, den Befehl mit STRG-C zu beenden und den Befehl dann erneut auszuführen, treten die gleichen Zeitverzögerungen und Sperren auf.

In der folgenden Tabelle werden die Optionen und Argumente für `infacmd ccps deleteClusters` beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-CloudProvisioningConfigurationID -cpcid	cloud_provisioning_configuration_id	Erforderlich. ID der Cloud-Bereitstellungskonfiguration.
-ClusterIDs -cids	cluster_ids	Erforderlich. Durch Kommas getrennte Liste der zu löschenden Cluster.  Die Cluster-ID entspricht der Cluster-ID, die auf der Website der Cloud-Plattform aufgeführt ist.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ConfigurationName -cn	Name der Cluster-Konfiguration	Erforderlich. Name der Cluster-Konfiguration in der Domäne. Bei Werten wird die Groß- und Kleinschreibung nicht beachtet.
-DeleteConnections -dc	delete_associated_connection	Optional. Löscht die Verbindungen, die von der Cluster-Konfiguration erstellt wurden. Verwenden Sie einen der folgenden Werte: - TRUE - FALSE Standardwert ist FALSE.

## listClusters

Listet die Cluster auf, die der Cluster-Arbeitsablauf erstellt und die auf der Cloud-Plattform vorhanden sind.

Der Befehl „infacmd ccps listClusters“ verwendet die folgende Syntax:

```
listClusters
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
<-CloudProvisioningConfigurationID|-cpcid> cloud_provisioning_configuration_id
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für `infacmd ccps listClusters` beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
- CloudProvisioningConfigurationID -cpcid	cloud_provisioning_configuration_id	Erforderlich. ID der Cloud-Bereitstellungskonfiguration.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.</p>

## updateADLSCertificate

Aktualisiert den Prinzipalzertifikatpfad des Azure Data Lake-Diensts in einer Cloud-Bereitstellungskonfiguration.

Der Befehl „infacmd ccps updateADLSCertificate“ verwendet die folgende Syntax:

```
updateADLSCertificate
  <-DomainName|-dn> domain_name
  <-UserName|-un> user_name
  <-Password|-pd> password
  <-CloudProvisioningConfigurationID|-cpcid> cloud_provisioning_configuration_id
  <-CertificateFilePath|-certPath> certificate_file_path
  [<-SecurityDomain|-sdn> security_domain]
  [<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für `infacmd ccps updateADLSCertificate` beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
- CloudProvisioningConfigurationID -cpcid	cloud_provisioning_configuration_id	Erforderlich. ID der Cloud-Bereitstellungskonfiguration, die mit dem Zertifikatdateipfad aktualisiert werden soll.
-CertificateFilePath -certPath	certificate_file_path	Erforderlich. Pfad zum ADLS-Dienstprinzipalzertifikat auf dem Datenintegrationsdienst-Computer.



Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.</p>

# KAPITEL 11

## infacmd cluster-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [createConfiguration, 102](#)
- [createConfigurationWithParams, 105](#)
- [deleteConfiguration, 107](#)
- [clearConfigurationProperties, 109](#)
- [exportConfiguration, 111](#)
- [listAssociatedConnections, 113](#)
- [listConfigurationGroupPermissions, 115](#)
- [listConfigurationSets, 117](#)
- [listConfigurationProperties, 118](#)
- [listConfigurations, 120](#)
- [listConfigurationUserPermissions, 122](#)
- [refreshConfiguration, 123](#)
- [setConfigurationPermissions, 125](#)
- [setConfigurationProperties, 127](#)
- [updateConfiguration, 129](#)

### createConfiguration

Imports cluster information directly from a cluster or from a cluster archive file.

The cluster configuration is an object in the domain that contains configuration information about the compute cluster.

The infacmd cluster createConfiguration command uses the following syntax:

```
createConfiguration
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
[<-DistributionType|-dt> CDH|EMR|HDI|HDP|MAPR|DATAPROC|DATABRICKS]
[<-DistributionVersion|-dv> distribution_version]
[<-ClusterManagerUri|-uri> cluster_manager_uri]
[<-ClusterManagerUser|-cmu> cluster_manager_user]
```

```
[<-ClusterManagerPassword|-cmp> cluster_manager_password]
[<-ClusterName|-cln> cluster_name]
[<-FilePath|-path> file_path]
[<-createConnections|-cc> true|false]
```

The following table describes infacmd cluster createConfiguration options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication or if you import properties directly from the cluster. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description
-ConfigurationName -cn	Name of the cluster configuration	Required. The cluster configuration name must meet the following requirements: <ul style="list-style-type: none"> <li>- Unique within the domain</li> <li>- Cannot exceed 128 characters</li> <li>- Cannot contain white spaces or the following special characters: <ul style="list-style-type: none"> <li>- ~ ` ! \$ % ^ &amp; * ( ) - + = { [ ] }   \ : ; " ' &lt; , &gt; . ? /</li> </ul> </li> </ul> Values are not case sensitive.
-DistributionType -distType	Distribution	Required. One of the following distribution types: <ul style="list-style-type: none"> <li>- CDH. Cloudera CDH or Cloudera CDP.</li> <li>- EMR. Amazon EMR.</li> <li>- HDI. Azure HDInsight.</li> <li>- HDP. Hortonworks HDP.</li> <li>- MAPR</li> <li>- DATAPROC</li> <li>- DATABRICKS</li> </ul> Values are not case sensitive.
-DistributionVersion -dv	Distribution version	Optional. Specify a distribution version other than the default version.  Each distribution has a default version. Use the -dv option to specify a different supported version to apply to the cluster configuration.  Default is the most recent distribution version that Data Engineering supports.
-ClusterManagerUri -uri	Cluster manager URI	Required to import directly from the cluster. URI of the cluster configuration web interface.
-ClusterManagerUser -cmu	Cluster Manager user	Required to import directly from the cluster. User name of the account to log in to the cluster configuration web interface.
-ClusterManagerPassword -cmp	Cluster Manager password	Required to import directly from the cluster. Password of the account to log in to the cluster configuration web interface.
-ClusterName -cln	Cluster name	Required if the cluster manager manages multiple clusters. If you do not provide a cluster name, the wizard imports information based on the default cluster.
-FilePath -path	Path and filename to the location of the archive file.	Required to import cluster information from a file. Path and file name of the archive file that contains cluster information.
-createConnections -cc	true/false	Optional. Indicates whether to create connections associated with the cluster configuration. Default is false.

# createConfigurationWithParams

Creates a cluster configuration through cluster parameters that you specify in the command line.

The cluster configuration is an object in the domain that contains configuration information about the compute cluster.

The infacmd cluster createConfigurationWithParams command uses the following syntax:

```
createConfigurationWithParams
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
<-DistributionType|-dt> CDH|EMR|HDI|HDP|MAPR|DATAPROC|DATABRICKS
[<-DistributionVersion|-dv> distribution_version]
<-Parameters|-params> parameters, separated by space in the form of name=value.
Use single quote to escape any equal sign or space in the value.
```

The following table describes infacmd cluster createConfigurationWithParams options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication or if you import properties directly from the cluster. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConfigurationName -cn	Name of the cluster configuration	Required. The cluster configuration name must meet the following requirements: <ul style="list-style-type: none"> <li>- Unique within the domain</li> <li>- Cannot exceed 128 characters</li> <li>- Cannot contain white spaces or the following special characters:  ~ ` ! \$ % ^ &amp; * ( ) - + = { [ ]   \ : ; " ' &lt; , &gt; . ? /</li> </ul> Values are not case sensitive.
-DistributionType -distType	Distribution	Required. One of the following distribution types: <ul style="list-style-type: none"> <li>- CDH. Cloudera CDH or Cloudera CDP.</li> <li>- EMR. Amazon EMR.</li> <li>- HDI. Azure HDInsight.</li> <li>- HDP. Hortonworks HDP.</li> <li>- MAPR</li> <li>- DATAPROC</li> <li>- DATABRICKS</li> </ul> Values are not case sensitive.

Option	Argument	Description
-DistributionVersion -dv	Distribution version	Optional. Specify a distribution version other than the default version.  Each distribution has a default version. Use the -dv option to specify a different supported version to apply to the cluster configuration.  Default is the most recent distribution version that Big Data Management supports.
-Parameters -params	Parameters	Separated by space in the form of name=value. Use single quote to escape any equal sign or space in the value.  You can use the following parameters for each distribution : <ul style="list-style-type: none"> <li>- Databricks: <ul style="list-style-type: none"> <li>- url</li> <li>- accesstoken</li> <li>- clusterid</li> </ul> </li> <li>- All other distribution types: <ul style="list-style-type: none"> <li>- host</li> <li>- port</li> <li>- username</li> <li>- password</li> <li>- clustername</li> </ul> </li> </ul>

## deleteConfiguration

Löscht eine Cluster-Konfiguration aus der Domäne.

Sie können keine Cluster-Konfiguration löschen, die von einem beliebigen Verbindungsobjekt verwendet wird.

Der Befehl `infacmd cluster deleteConfiguration` verwendet die folgende Syntax:

```
deleteConfiguration
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
[<-DeleteConnections|-dc> delete_associated_connections]
```

In der folgenden Tabelle werden die Optionen und Argumente für `infacmd cluster deleteConfiguration` beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der <code>infacmd</code> versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet <code>infacmd</code> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.



Option	Argument	Beschreibung
-ConfigurationName -cn	Name der Cluster-Konfiguration	Erforderlich. Name der Cluster-Konfiguration in der Domäne. Bei Werten wird die Groß- und Kleinschreibung nicht beachtet.
-DeleteConnections -dc	delete_associated_connection	Optional. Legen Sie den Wert auf TRUE fest, um alle Verbindungen zu löschen, die der Cluster-Konfiguration zugeordnet sind. Standardwert ist FALSE.

## clearConfigurationProperties

Löscht überschriebene Eigenschaftswerte im Cluster-Konfigurationssatz.

Der Befehl löscht überschriebene Werte von importierten Eigenschaften und stellt den importierten Wert wieder her. Der Befehl löscht benutzerdefinierte Eigenschaften aus einem Konfigurationssatz. Verwenden Sie die Option -del, um eine importierte Eigenschaft zu löschen.

**Hinweis:** Wenn Sie eine importierte Eigenschaft löschen, wird die Eigenschaft bei der Aktualisierung wiederhergestellt, falls sie im Cluster vorhanden ist.

Der folgende Befehl löscht z. B. die benutzerdefinierten Eigenschaften „foo.bar“ und „biz.baz“ aus dem Satz in der Datei „core-site.xml“ der CDH1-Cluster-Konfiguration:

```
infacmd cluster clearConfigurationProperties -cn CDH1 -cs core-site.xml -pn foo.bar
biz.baz
```

Der Befehl „infacmd cluster clearConfigurationProperties“ verwendet die folgende Syntax:

```
clearConfigurationProperties
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
<-ConfigurationSet|-cs> configuration_set
<-PropertyNames|-pn> list of property names separated by space
[<-DeleteProperties|-del> delete_properties]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd cluster clearConfigurationProperties“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ConfigurationName -cn	Name der Cluster-Konfiguration	Erforderlich. Name der Cluster-Konfiguration in der Domäne. Bei Werten wird die Groß- und Kleinschreibung nicht beachtet.
-ConfigurationSet -cs	Konfigurationssatz	Name des Konfigurationssatzes. Geben Sie den Namen der XML-Konfigurationsdatei ein. Beispiel: hdfs-site.xml. Wenn Sie einen XML-Dateinamen eingeben, gibt der Befehl die Eigenschaften und Werte in diesem Konfigurationssatz zurück.
-PropertyNames -pn	property_name	Eigenschaften, für die der Befehl ausgeführt werden soll. Wenn Sie eine importierte Eigenschaft einschließen, löscht der Befehl einen Überschreibungswert. Wenn Sie eine benutzerdefinierte Eigenschaft einschließen, löscht der Befehl die Eigenschaft.  Um mehrere Eigenschaften zu bearbeiten, trennen Sie die Eigenschaftsnamen durch Leerzeichen.  Wenn die Eigenschaft keine benutzerdefinierte Eigenschaft ist, verwenden Sie die Option -del.
-DeleteProperties -del	delete_properties	Optional. Wenn Sie die Option auf TRUE festlegen, wird eine importierte Eigenschaft gelöscht. Standardwert ist FALSE.

## exportConfiguration

Exportiert eine Clusterkonfiguration in eine Datei, die XML-Dateien enthält, oder in eine kombinierte XML-Datei.

Exportieren Sie die Eigenschaften, die ein Cluster-Konfigurationsobjekt enthält, in eine komprimierte Datei in einem von Ihnen angegebenen Pfad.

Wenn Sie die Cluster-Konfigurationsdatei exportieren, erstellen Sie ein ZIP-Archiv.

Der Befehl „`infacmd cluster exportConfiguration`“ verwendet die folgende Syntax:

```
exportConfiguration
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
<-FilePath|-path> file_path
[<-IncludeSensitive|-is> include_sensitive_properties]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd cluster exportConfiguration“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ConfigurationName -cn	Name der Cluster-Konfiguration	Erforderlich. Name der Cluster-Konfiguration in der Domäne. Bei Werten wird die Groß- und Kleinschreibung nicht beachtet.
-FilePath -path	Pfad zum Speicherort der zu erstellenden Datei und deren Dateiname.	Erforderlich. Pfad und Dateiname der komprimierten Datei, die als Archiv der Cluster-Konfiguration erstellt werden soll. Sie können einen absoluten Pfad oder einen relativen Pfad für den Dateinamen angeben. Schließen Sie das Suffix <code>.zip</code> oder <code>.tar</code> ein.
-IncludeSensitive -is	include_sensitive_properties	Optional. Auf TRUE festgelegt, um vertrauliche Eigenschaften zu exportieren. Um sie in den Export einzuschließen, müssen Sie über Schreibberechtigungen für die Cluster-Konfiguration verfügen. Standardwert ist FALSE.

## listAssociatedConnections

Listet Verbindungen nach Typ auf, die der angegebenen Cluster-Konfiguration zugeordnet sind.

Der Befehl listet die Ergebnisse nach Verbindungstyp auf.

Der Befehl `infacmd cluster listAssociatedConnections` verwendet die folgende Syntax:

```
listAssociatedConnections
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
```

In der folgenden Tabelle werden die Optionen und Argumente für `infacmd cluster listAssociatedConnections` beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ConfigurationName -cn	Name der Cluster-Konfiguration	Erforderlich. Name der Cluster-Konfiguration in der Domäne. Bei Werten wird die Groß- und Kleinschreibung nicht beachtet.

## listConfigurationGroupPermissions

Listet die Berechtigungen auf, die eine Gruppe für eine Cluster-Konfiguration hat.

Die Befehlsausgabe umfasst Gruppenberechtigungen und die Sicherheitsdomäne, der die Gruppe angehört.

Der Befehl „infacmd cluster listConfigurationGroupPermissions“ verwendet die folgende Syntax:

```
listConfigurationGroupPermissions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
[<-Direct> direct]
[<-GroupFilter|-groups> group_filter]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd cluster listConfigurationGroupPermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ConfigurationName -cn	Name der Cluster-Konfiguration	Erforderlich. Name der Cluster-Konfiguration in der Domäne. Bei Werten wird die Groß- und Kleinschreibung nicht beachtet.
-Direct	Gibt an, ob direkte oder effektive Berechtigungen aufgelistet werden sollen.	Optional. Bestimmt, ob Sie Berechtigungen auflisten, die der Administrator der Cluster-Konfiguration direkt erteilt hat. Geben Sie einen dieser Werte an: - „Direct“. Die Berechtigungen, die der Administrator der Gruppe direkt erteilt hat. - „Effective“. Alle Berechtigungen, die die Gruppe hat, einschließlich der direkten und geerbten Berechtigungen. Standardwert ist „Effective“.
GroupFilter -groups	Gruppenfilter	Optional. Listet die Gruppe(n) auf, für die Ergebnisse angezeigt werden sollen. Wenn Sie keine Gruppe angeben, zeigt der Befehl standardmäßig die Ergebnisse für alle Gruppen an. Trennen Sie Gruppennamen durch Leerzeichen.



# listConfigurationSets

Listet die Konfigurationseinstellungen auf, die eine Cluster-Konfiguration enthält.

Der Befehl „infacmd cluster listConfigurationSets“ verwendet die folgende Syntax:

```
listConfigurationSets
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd cluster listConfigurationSets“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.</p>
-ConfigurationName -cn	Name der Cluster-Konfiguration	<p>Erforderlich. Name der Cluster-Konfiguration in der Domäne. Bei Werten wird die Groß- und Kleinschreibung nicht beachtet.</p>

## listConfigurationProperties

Listet Eigenschaften und aktive Werte für einen Konfigurationssatz auf.

Der Befehl „infacmd cluster listConfigurationProperties“ verwendet die folgende Syntax:

```
listConfigurationProperties
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
<-ConfigurationSet|-cs> configuration_set
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd cluster listConfigurationProperties“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ConfigurationName -cn	Name der Cluster-Konfiguration	Erforderlich. Name der Cluster-Konfiguration in der Domäne. Bei Werten wird die Groß- und Kleinschreibung nicht beachtet.
-ConfigurationSet -cs	Konfigurationssatz	Name des Konfigurationssatzes. Geben Sie eine der folgenden Konfigurationssatzoptionen ein: <ul style="list-style-type: none"> <li>- allgemein. Wenn Sie diese Option eingeben, gibt der Befehl die Eigenschaftswerte in der Kategorie „Allgemein“ der Cluster-Konfigurationsoptionen zurück: <ul style="list-style-type: none"> <li>- Beschreibung</li> <li>- Distributionstyp</li> <li>- Versionsnummer</li> <li>- Zeitpunkt der letzten Aktualisierung</li> </ul> </li> <li>- Name der XML-Konfigurationsdatei. Beispiel: hdfs-site.xml. Wenn Sie einen XML-Dateinamen eingeben, gibt der Befehl die Eigenschaften und Werte in diesem Konfigurationssatz zurück.</li> </ul>

## listConfigurations

Listet die Cluster-Konfigurationen in der Domäne auf.

Der Befehl „`infacmd cluster listConfigurations`“ verwendet die folgende Syntax:

```
listConfigurations
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd cluster listConfigurations“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

# listConfigurationUserPermissions

Lists the permissions that a user has for a cluster configuration.

The infacmd cluster listConfigurationUserPermissions command uses the following syntax:

```
listConfigurationUserPermissions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
[<-Direct> direct]
[<-UserFilter|-users> user_filter]
```

The following table describes infacmd cluster listConfigurationUserPermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.  If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConfigurationName -cn	Name of the cluster configuration	Required. Name of the cluster configuration on the domain. Values are not case sensitive.
-Direct	Whether to list direct or effective permissions.	Optional. Determines whether you list permissions that the administrator has directly granted to the cluster configuration. Specify one of these values: <ul style="list-style-type: none"> <li>- Direct. The permissions that the administrator directly granted to the group.</li> <li>- Effective. All of the permissions that the group has, including direct and inherited permissions.</li> </ul> Default is effective.
UserFilter -users	user_filter	Optional. List the user or users to show results for. If you do not specify a user, the command displays results for all users by default. Values are not case sensitive.

## refreshConfiguration

Aktualisiert eine Cluster-Konfiguration aus einer Cluster-Archivdatei oder aus einem ausgelagerten Cluster-Manager. Änderungen werden wirksam, nachdem Sie den Datenintegrationsdienst neu gestartet haben.

Aktualisiert die Cluster-Konfigurationseigenschaften aus einem Cluster oder aus einer Cluster-Archivdatei. Mit dem Befehl „refreshConfiguration“ werden die importierten Konfigurationswerte aktualisiert. Er wirkt sich nicht auf die von Ihnen konfigurierten Überschreibungen aus.

Der Befehl „infacmd cluster refreshConfiguration“ verwendet die folgende Syntax:

```
refreshConfiguration
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
[<-ClusterManagerUri|-uri> cluster_manager_uri]
[<-ClusterManagerUser|-cmu> cluster_manager_user]
[<-ClusterManagerPassword|-cmp> cluster_manager_password]
[<-ClusterManagerName|-cmn> cluster_name]
[<-FilePath|-path> file_path]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd cluster refreshConfiguration“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.



Option	Argument	Beschreibung
-ConfigurationName -cn	Name der Cluster-Konfiguration	Erforderlich. Name der Cluster-Konfiguration in der Domäne. Bei Werten wird die Groß- und Kleinschreibung nicht beachtet.
-ClusterManagerUri -uri	Cluster-Manager-URI	Erforderlich für den direkten Import aus dem Cluster. URI der Webschnittstelle der Cluster-Konfiguration.
-ClusterManagerUser -cmu	Cluster-Manager-Benutzer	Erforderlich für den direkten Import aus dem Cluster. Benutzername des Kontos, über das die Anmeldung bei der Webschnittstelle der Cluster-Konfiguration erfolgen soll.
-ClusterManagerPassword -cmp	Cluster-Manager-Passwort	Erforderlich für den direkten Import aus dem Cluster. Passwort des Kontos, über das die Anmeldung bei der Webschnittstelle der Cluster-Konfiguration erfolgen soll.
-ClusterName -cln	Name des Clusters	Erforderlich, wenn der Cluster-Manager mehrere Cluster verwaltet. Wenn Sie keinen Cluster-Namen angeben, importiert der Assistent Informationen basierend auf dem Standard-Cluster.
-FilePath -path	Pfad zum Speicherort der Archivdatei und deren Dateiname.	Erforderlich, um Cluster-Informationen aus einer Datei zu importieren. Pfad und Dateiname der Archivdatei, die Cluster-Konfigurationsdateien vom Typ „*-site.xml“ enthält.

## setConfigurationPermissions

Legt Berechtigungen zur Cluster-Konfiguration für einen Benutzer oder eine Gruppe nach dem Entfernen der vorherigen Berechtigungen fest.

Sie können damit Cluster-Konfigurationsberechtigungen für einen Benutzer oder eine Gruppe hinzufügen, ändern oder löschen. Entfernt frühere Berechtigungen für den Benutzer oder die Gruppe.

Verwenden Sie entweder die Option `-RecipientUserName` oder `-RecipientGroupName`.

Sie können in einem einzigen Befehl mehrere der folgenden Berechtigungen gewähren: READ, WRITE, EXECUTE, GRANT. Nur ALL oder NONE kann separat gewährt werden.

Der Befehl „`infacmd cluster setConfigurationPermissions`“ verwendet die folgende Syntax:

```
setConfigurationPermissions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
<<-RecipientUserName|-run> recipient_user_name | <-RecipientGroupName|-rgn>
recipient_group_name>>
[<-RecipientSecurityDomain|-rsd> recipient_security_domain]
<-Permissions|-p> READ_WRITE_EXECUTE_GRANT|ALL|NONE
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd cluster setConfigurationPermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ConfigurationName -cn	Name der Cluster-Konfiguration	Erforderlich. Name der Cluster-Konfiguration in der Domäne. Bei Werten wird die Groß- und Kleinschreibung nicht beachtet.
-RecipientUserName -run	recipient_user_name	Erforderlich, wenn Sie nicht die Option RecipientGroupName verwenden. Name des Benutzers, dem die Berechtigung gewährt werden soll.
-RecipientGroupName -rgn	recipient_group_name	Erforderlich, wenn Sie nicht die Option RecipientUserName verwenden. Name der Gruppe, der die Berechtigung gewährt werden soll.
-RecipientSecurityDomain -rsd	recipient_security_domain	Sicherheitsdomäne, der der Benutzer oder die Gruppe angehört.
-Permissions -p	READ   WRITE   EXECUTE   GRANT ALL NONE	Zu erteilende Berechtigung(en). Um mehr als eine Berechtigung einzugeben, trennen Sie die Berechtigungen durch ein Leerzeichen.

## setConfigurationProperties

Fügt benutzerdefinierte Eigenschaften hinzu oder überschreibt importierte Eigenschaftswerte.

Der Befehl `infacmd cluster setConfigurationProperties` verwendet die folgende Syntax:

```
setConfigurationProperties
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
<-ConfigurationSet|-cs> configuration_set
<-UserProperties|-up> user_properties_separated_by_&:
```

In der folgenden Tabelle werden die Optionen und Argumente für setConfigurationProperties beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ConfigurationName -cn	Name der Cluster-Konfiguration	Erforderlich. Name der Cluster-Konfiguration in der Domäne. Bei Werten wird die Groß- und Kleinschreibung nicht beachtet.

Option	Argument	Beschreibung
-ConfigurationSet -cs	Konfigurationssatz	Name des Konfigurationssatzes. Geben Sie den Namen der XML-Konfigurationsdatei ein. Beispiel: hdfs-site.xml. Wenn Sie einen XML-Dateinamen eingeben, gibt der Befehl die Eigenschaften und Werte in diesem Konfigurationssatz zurück.
-UserProperties -up	Festzulegende Benutzereigenschaften	Name-Wert-Paare für Eigenschaften. Verwenden Sie zur Begrenzung der Eigenschaft-Wert-Paare das Gleichheitszeichen (=). Trennen Sie die einzelnen Paare mit den Zeichen & : voneinander.

## -UserProperties Examples

In den folgenden Beispielen wird dargestellt, wie Sie eine einzelne Benutzereigenschaft oder mehrere Eigenschaft-Wert-Paare hinzufügen oder eine Benutzereigenschaft überschreiben:

### Einzelne Benutzereigenschaft hinzufügen

Zum Hinzufügen einer einzelnen Benutzereigenschaft verwenden Sie das Gleichheitszeichen zur Begrenzung von Eigenschaft-Wert-Paaren. Der folgende Befehl fügt z. B. dem core-site.xml-Namespace der Cluster-Konfiguration die Eigenschaft foo.bar hinzu und weist foo.bar einen Wert von 1 zu:

```
infacmd cluster setConfigurationProperties -cn cdh -cs core-site.xml -up 'foo.bar=1'
```

### Mehrere Eigenschaft-Wert-Paare hinzufügen

Begrenzen Sie Eigenschaft-Wert-Paare mit dem Gleichheitszeichen (=) und trennen Sie Paare mit &:. Der folgende Befehl fügt dem Namespace „core-site.xml“ der Cluster-Konfiguration die Eigenschaft „foo.bar“ hinzu und weist „foo.bar“ einen Wert von 1 zu. Anschließend wird demselben Namespace die Eigenschaft „start.interval“ hinzugefügt und „start.interval“ wird der Wert 5 zugewiesen.

```
infacmd cluster setConfigurationProperties -cn cdh -cs core-site.xml -up 'foo.bar=1&:start.interval=5'
```

### Benutzereigenschaft überschreiben

Zum Überschreiben des Werts einer Eigenschaft geben Sie das Eigenschaft-Wert-Paar mit einem anderen Wert an. Der folgende Befehl bearbeitet beispielsweise die vorhandene Eigenschaft fs.trash.interval im core-site.xml-Namespace der Cluster-Konfiguration. Der Befehl überschreibt den vorhandenen Wert und weist den Wert 2 zu:

```
infacmd cluster setConfigurationProperties -cn cdh -cs core-site.xml -up 'fs.trash.interval=2'
```

# updateConfiguration

Aktualisiert die Hadoop-Distributionsversion einer Cluster-Konfiguration.

Verwenden Sie die Option -dv, um die Distributionsversion der Hadoop-Distribution einer Cluster-Konfiguration zu ändern.

Der Befehl „infacmd cluster updateConfiguration“ verwendet die folgende Syntax:

```
updateConfiguration
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
<-DistributionVersion|-dv> distribution_version
```

In der folgenden Tabelle werden die Optionen und Argumente für `infacmd cluster updateConfiguration` beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ConfigurationName -cn	Name der Cluster-Konfiguration	Erforderlich. Name der Cluster-Konfiguration in der Domäne. Bei Werten wird die Groß- und Kleinschreibung nicht beachtet.
-DistributionVersion -dv	Distributionsversion, in die gewechselt werden soll.	Erforderlich. Geben Sie eine andere Distributionsversion für eine Cluster-Konfiguration an. Wenn z. B. die standardmäßig unterstützte Version der Hadoop-Distribution 5.13 ist, der Cluster jedoch Version 5.12 besitzt, geben Sie 5.12 an.

# KAPITEL 12

## infacmd cms-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [CreateAuditTables, 132](#)
- [CreateService, 134](#)
- [DeleteAuditTables, 137](#)
- [ListServiceOptions, 139](#)
- [ListServiceProcessOptions, 141](#)
- [Löschen, 143](#)
- [RemoveService, 145](#)
- [ResyncData, 147](#)
- [UpdateServiceOptions, 149](#)
- [UpdateServiceProcessOptions, 152](#)
- [Upgrade, 154](#)

### CreateAuditTables

Erstellt Audit-Tabellen, die Audit-Trail-Protokollereignisse für Referenztabellen enthalten, die vom angegebenen Content-Managementdienst verwaltet werden.

Der Befehl „infacmd cms CreateAuditTables“ verwendet die folgende Syntax:

```
CreateAuditTables
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```



In der folgenden Tabelle werden die Optionen und Argumente für „infacmd cms CreateAuditTables“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Content-Managementdienst.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang..

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie den Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## CreateService

Erstellt einen Content-Managementdienst in einer Domäne.

Der Befehl „infacmd cms CreateService“ verwendet die folgende Syntax:

```

CreateService

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

<-DataServer|-ds> data_service_name

<-RepositoryService|-rs> repository_service_name

<-RepositoryUsername|-rsu> repository_user_name

<-RepositoryPassword|-rsp> repository_password

```

```
[<-RepositorySecurityDomain|-rssd> repository_security_domain]

<-ReferenceDataLocation|-rdl> reference_data_location

[<-HttpPort> http_port]

[<-HttpsPort> https_port]

[<-KeystoreFile|-kf> keystore_file_location]

[<-KeystorePassword|-kp> keystore_password]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd cms CreateService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Content-Managementdienst. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf nicht länger als 128 Zeichen sein und keine führenden oder abschließenden Leerzeichen, Wagenrückläufe, Tabulatoren oder die folgenden Zeichen enthalten:  / * ? < > "
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang. Standardwert ist „180 Sekunden“.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Content-Managementdienst ausgeführt wird.
-DataServer -ds	data_service_name	Erforderlich. Der mit dem Content-Managementdienst verbundene Name des Datenintegrationsdiensts.
-RepositoryService -rs	repository_service_name	Erforderlich. Modellrepository-Dienst für die Verknüpfung mit den Content-Managementdienst.
-RepositoryUsername -rsu	repository_user_name	<p>Erforderlich. Benutzername für die Verbindung mit dem Modellrepository-Dienst.</p> <p>Um Aufgaben zur Verwaltung von Referenztabellen im Modellrepository durchzuführen, muss der in der Eigenschaft angegebene Benutzer über eine Administratorrolle für den Modellrepository-Dienst verfügen. Die Aufgaben zur Verwaltung von Referenztabellen umfassen das Löschen von verwaisten Referenztabellen.</p>
-RepositoryPassword -rsp	repository_password	Erforderlich. Passwort für die Verbindung zum Modellrepository-Dienst.
-RepositorySecurityDomain -rssd	repository_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Native“.

Option	Argument	Beschreibung
-ReferenceDataLocation -rdl	reference_data_location	Erforderlich. Verbindungsname für die Datenbank, die Datenwerte für die im Modellrepository definierten Referenztabellen speichert. Die angegebene Datenbank speichert Referenzdatenwerte. Das Modellrepository speichert Metadaten für die Referenztabellen.
-HttpPort	http_port	Erforderlich. Eindeutige HTTP-Portnummer für den Content-Managementdienst.
-HttpsPort	https_port	Optional. HTTPS-Portnummer, an der der Dienst ausgeführt wird, wenn Sie das TLS-Protokoll (Transport Layer Security) aktivieren.
-KeystoreFile -kf	keystore_file_location	Pfad und Dateiname der Schlüsselspeicherdatei mit den Schlüsseln und Zertifikaten, die zur Aktivierung von TLS und zur Verwendung des HTTPS-Protokolls für den Dienst erforderlich sind.
- KeystorePassword> -kp	keystore_password	Erforderlich, wenn Sie TLS aktivieren und HTTPS-Verbindungen für den Dienst verwenden. Ein Klartextpassword für die Schlüsselspeicherdatei.

## DeleteAuditTables

Löscht die Audit-Trail-Tabellen für den angegebenen Content-Managementdienst.

Der Befehl „infacmd cms DeleteAuditTables“ verwendet die folgende Syntax:

```

DeleteAuditTables
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd cms DeleteAuditTables“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Content-Managementdienst.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang..

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie den Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## ListServiceOptions

Listet die Optionen für einen Content Management Service auf.

Der Befehl `infacmd cms ListServiceOptions` verwendet die folgende Syntax:

```
ListServiceOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden infacmd cms ListServiceOptions-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Content-Managementdienst.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang..



Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie den Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## ListServiceProcessOptions

Listet die Optionen für einen Content-Managementdienst-Prozess auf.

Der Befehl „infacmd cms ListServiceProcessOptions“ verwendet die folgende Syntax:

```
ListServiceProcessOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

Die folgende Tabelle beschreibt s cms ListServiceProcessOptions-Optionen und -Argumente:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Content-Managementdienst.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie den Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienstprozess ausgeführt wird.

## Löschen

Löscht aus dem Referenzdaten-Warehouse alle Referenztabellen, die keinem Referenztabellenobjekt im Modellrepository mehr zugeordnet sind.

Beim Ausführen von `infacmd cms Purge` erkennt der Content-Management-Dienst die Tabellen, die Daten für Referenztabellenobjekte im zugehörigen Modellrepository speichern. Der Content-Management-Dienst löscht alle anderen Tabellen aus dem Warehouse und erzeugt eine Liste der gelöschten Tabellen. Führen Sie `infacmd cms Purge` im Master-Content-Management-Dienst für das Modellrepository aus.

**Hinweis:** Zur Vermeidung eines versehentlichen Datenverlusts werden während des Löschvorgangs Tabellen nur dann gelöscht, wenn das Modellrepository ein Referenztabellenobjekt enthält.

Überprüfen Sie vor dem Ausführen von `infacmd cms Purge` die folgenden Voraussetzungen:

- Der im Befehl angegebene Benutzername verfügt über die Berechtigung zum Verwalten von Diensten in der Domäne.
- Der vom Content-Management-Dienst angegebene Modellrepository-Benutzer weist im Modellrepository-Dienst die Administratorrolle auf.
- Alle Datenintegrationsdienste, die mit dem Modellrepository verbunden sind, stehen zur Verfügung.
- Im Referenzdaten-Warehouse finden aktuell keine Datenvorgänge statt.
- Das Referenzdaten-Warehouse speichert Daten für die Referenztabellenobjekte in einem einzelnen Modellrepository.

Der Befehl „`infacmd cms Purge`“ verwendet die folgende Syntax:

```
Purge
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd cms Purge“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Content-Management-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf nicht länger als 128 Zeichen sein und keine führenden oder abschließenden Leerzeichen, Wagenrückläufe, Tabulatoren oder die folgenden Zeichen enthalten:  / * ? < > "
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang. Standardwert ist 180 Sekunden.</p>

## RemoveService

Entfernt den Content-Managementdienst aus der Domäne. Bevor Sie einen Dienst entfernen, müssen Sie ihn deaktivieren.

Der Befehl „infacmd cms RemoveService“ verwendet die folgende Syntax:

```
RemoveService
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd cms RemoveService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des zu entfernenden Diensts. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

# ResyncData

Synchronisiert probabilistische Modelldateien oder klassifizierende Modelldateien zwischen einem angegebenen Content-Managementdienst-Rechner und dem Master-Content-Managementdienst-Rechner in der Domäne. Mit dem Befehl ResyncData aktualisieren Sie die Dateien auf dem angegebenen Content-Managementdienst-Rechner mit den Dateien vom Master-Content-Managementdienst-Rechner.

Der Befehl synchronisiert alle Dateien, die auf dem Master-Content-Managementdienst-Rechner gespeichert sind, nach einer von Ihnen angegebenen Zeit und Datum. Führen Sie den Befehl ResyncData für einen einzelnen Modelldateityp aus. Um probabilistische Modelldateien und klassifizierende Modelldateien zu synchronisieren, müssen Sie den Befehl zweimal ausführen.

Wenn Sie „infacmd cms ResyncData“ ausführen, müssen Sie über Zugriffsberechtigungen auf beiden Content-Managementdienst-Rechnern verfügen. Informatica Administrator legt die Zugriffsberechtigungen auf die Dienste fest.

Der Befehl „infacmd cms ResyncData“ verwendet die folgende Syntax:

```
ResyncData
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Type|-t> type
<-StartTime|-st> start_time
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd cms resyncData“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Content-Managementdienst. Der Befehl kopiert Dateien auf den Rechner, der den Dienst hostet.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	Passwort	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p> <p>.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie den Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>



Option	Argument	Beschreibung
-Type -t	type	Erforderlich. Identifiziert den Datendateityp zum Kopieren vom Master-Content-Managementdienst-Rechner aus. Geben Sie eine der folgenden Optionen ein: - NER. Gibt probabilistische Modelldatendateien an. - Klassifizierer. Gibt klassifizierende Modelldatendateien an.
-StartTime -st	start_time	Erforderlich. Identifiziert die Dateien zum Kopieren vom Master-Content-Managementdienst-Rechner auf den Content-Managementdienst-Rechner, den Sie in der Eigenschaft ServiceName angeben. Mit dem Befehl werden nur Dateien kopiert, die einen späteren Zeitstempel als den Wert StartTime haben. Der Befehl verwendet die Systemuhr im Master-Content-Managementdienst-Rechner, um die Uhrzeit festzustellen.  Geben Sie das Datum im lokalen Standardformat ein.

## UpdateServiceOptions

Aktualisiert den Content-Managementdienst mit Optionen, die in der aktuellen Version eingeführt wurden. Um die aktuellen Optionen anzuzeigen, führen Sie den Befehl `infacmd cms ListServiceOptions` aus.

Der Befehl „`infacmd cms UpdateServiceOptions`“ verwendet die folgende Syntax:

```
UpdateServiceOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd cms UpdateServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Content-Management-Diensts.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Options -o	options	Erforderlich. Geben Sie alle zu aktualisierenden Optionen und Werte ein. Trennen Sie die einzelnen Optionen durch ein Leerzeichen. Zum Anzeigen der Anwendungsoptionen führen Sie den Befehl „infacmd cms ListServiceOptions“ aus.

## Benutzername- und Passwort-Optionen

Sie können die Option -o für UpdateServiceProcessOptions verwenden, um den Benutzernamen und das Passwort zu aktualisieren, welche der Content-Managementdienst nutzt, um eine Verbindung zum Modellrepository-Dienst herzustellen.

Verwenden Sie die Optionen „RepositoryUsername“ und „DataServiceOptions.RepositoryPassword“ zum Aktualisieren der Werte von Benutzername und Passwort. Sie können die Eigenschaften auch in Informatica Administrator einstellen.

## Referenzdaten-Optionen

Sie können die Option -o für UpdateServiceOptions verwenden, um die folgenden Verzeichnis- und Datenbankeneinstellungen für Referenzdaten zu aktualisieren:

- Mit der Option „FileTransferOptions.TempLocation“ identifizieren Sie das Stagingverzeichnis der Referenzdaten. Der Content-Managementdienst verwendet das Verzeichnis zum Staging von Daten, das er einer Referenztabelle hinzufügt.
- Mit der Option „DataServiceOptions.ReferenceDataLocation“ identifizieren Sie die Verbindung zur Referenzdaten-Datenbank. Die Referenzdaten-Datenbank speichert die Werte für die Referenztabelle, die Sie im Modellrepository auswählen können.
- Mit der Option „DataServiceOptions.RefDataLocationSchema“ geben Sie das Schema an, das die Referenzdatentabellen in der Datenbank der Referenzdaten identifiziert.

Wenn Sie kein Referenzdatenschema für den Content-Management-Dienst angeben, verwendet der Dienst das Schema, das von der Datenbankverbindung angegeben wird. Wenn Sie kein Schema für den Content-Management-Dienst oder die Datenbankverbindung angeben, greift der Dienst auf das Standarddatenbankschema zurück.

Sie können die Eigenschaften auch in Informatica Administrator einstellen.

**Hinweis:** Legen Sie die Datenbank und das Schema fest, die der Content-Management-Dienst für Referenzdaten verwendet, bevor Sie eine verwaltete Referenztabelle erstellen.

# UpdateServiceProcessOptions

Aktualisiert die Optionen für einen Content-Managementdienst-Prozess. Führen Sie zum Anzeigen der aktuellen Optionen den `infacmd cms ListServiceProcessOptions`-Befehl aus.

Der Befehl „`infacmd cms UpdateServiceProcessOptions`“ verwendet die folgende Syntax:

```
UpdateServiceProcessOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd cms UpdateServiceProcessOptions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Content-Management-Diensts.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienstprozess ausgeführt wird.
-Options -o	options	Erforderlich. Geben Sie alle zu aktualisierenden Optionen und Werte ein. Trennen Sie die einzelnen Optionen durch ein Leerzeichen. Zum Anzeigen der Anwendungsoptionen führen Sie den Befehl „infacmd cms ListServiceProcessOptions“ aus.

## Optionen für Identitätsvergleichsanalyse

Sie können die Option UpdateServiceProcessOptions -o verwenden, um die folgenden Eigenschaften für die Identitätsvergleichsanalyse zu aktualisieren:

- IdentityOptions.IdentityReferenceDataLocation. Gibt den Speicherort von Identitätspopulations-Dateien an.
- IdentityOptions.IdentityCacheDir. Gibt den Speicherort des Cache-Verzeichnisses an, das zur Identitätsvergleichsanalyse verwendet wird.
- IdentityOptions.IdentityIndexDir. Gibt den Speicherort des Index-Schlüsselverzeichnisses an, der in der Identitätsvergleichsanalyse verwendet wurde.

Sie können die Eigenschaften auch im Informatica Administrator einstellen.

# Upgrade

Aktualisiert die Content Management Service-Konfiguration. Führen Sie ein `infacmd cms Upgrade` aus, wenn Sie ein Upgrade auf die aktuelle Version von Informatica Data Quality durchführen.

Der Befehl `infacmd cms Upgrade` verwendet die folgende Syntax:

```
Upgrade

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

Der Befehl `infacmd cms Upgrade` prüft die Dienstkonfiguration auf der Domäne und überprüft die folgenden Dienstoptionen:

## Master-Content Management Service

Der Upgrade-Befehl überprüft, dass das Modellrepository in der Domäne einen Master-Content Management Service verwendet. Wenn der Model Repository Service keinen Master-Content Management Service angibt, dann stellt der Upgrade Befehl den aktuellen Dienst als Master-Content Management Service ein. Standardmäßig wird der erste Content Management Service, der sich mit einem Model Repository Service verbindet, zum Master-Content Management Service.

## Model Repository Service

Der Upgrade-Befehl verwendet den Data Integration Service, der mit dem Content Management Service verbunden ist, um den Model Repository Service in der Domäne zu ermitteln.

Der Upgrade-Befehl überprüft, ob der Content Management Service einen gültigen Benutzernamen, ein gültiges Passwort und eine Sicherheitsdomäne hat, um eine Verbindung zum Model Repository Service herzustellen. Wenn diese Optionen sind nicht eingestellt sind, verwendet der Upgrade-Befehl die Werte von Benutzernamen, Passwort und Sicherheitsdomäne im verbundenen Data Integration Service, um eine Verbindung zum Model Repository Service herzustellen.

## Referenzdaten-Speicherort

Der Upgrade-Befehl überprüft, ob der Content Management Service einen Referenzdaten-Speicherort angibt. Wenn der Dienst keinen Referenzdaten-Speicherort angibt, stellt der Upgrade-Befehl den Speicherort auf die Staging-Datenbank ein, die im Analyst Service definiert ist.

In der folgenden Tabelle werden `infacmd cms Upgrade`-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Content-Managementdienst.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	Passwort	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang..</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie den Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

# KAPITEL 13

## infacmd dis-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [AddParameterSetEntries, 157](#)
- [BackupApplication, 159](#)
- [CancelDataObjectCacheRefresh, 161](#)
- [CreateService, 163](#)
- [compareMapping, 166](#)
- [compareObject, 170](#)
- [DeleteParameterSetEntries, 174](#)
- [deployObjectsToFile, 177](#)
- [DeployApplication, 181](#)
- [disableMappingValidationEnvironment, 183](#)
- [enableMappingValidationEnvironment, 187](#)
- [ListApplicationObjectPermissions, 191](#)
- [ListApplicationObjects, 193](#)
- [ListApplicationOptions, 195](#)
- [ListApplicationPermissions, 197](#)
- [ListApplications, 199](#)
- [ListComputeOptions, 200](#)
- [ListDataObjectOptions, 202](#)
- [ListMappingEngines, 204](#)
- [ListParameterSetEntries, 207](#)
- [ListParameterSetObjects, 209](#)
- [ListParameterSets, 211](#)
- [listPatchNames, 212](#)
- [ListSequenceObjectProperties, 214](#)
- [ListSequenceObjects, 216](#)
- [ListServiceProcessOptions, 217](#)
- [PurgeDataObjectCache, 219](#)
- [PurgeResultSetCache, 221](#)
- [queryDesignTimeObjects, 223](#)
- [queryRunTimeObjects, 225](#)



- [RefreshDataObjectCache, 227](#)
- [RenameApplication, 228](#)
- [replaceMappingHadoopRuntimeConnections, 230](#)
- [RestoreApplication, 233](#)
- [SetApplicationPermissions, 234](#)
- [SetApplicationObjectPermissions, 237](#)
- [setMappingExecutionEnvironment, 239](#)
- [SetSequenceState, 241](#)
- [StartApplication, 244](#)
- [StopApplication, 246](#)
- [stopBlazeService, 248](#)
- [Tag, 251](#)
- [UndeployApplication, 259](#)
- [UpdateApplication, 261](#)
- [UpdateApplicationOptions, 263](#)
- [UpdateComputeOptions, 264](#)
- [UpdateDataObjectOptions, 266](#)
- [UpdateParameterSetEntries, 269](#)
- [UpdateServiceOptions , 271](#)
- [UpdateServiceProcessOptions , 285](#)
- [Regeln und Richtlinien, 289](#)

## AddParameterSetEntries

Fügt einem Parametersatz Einträge hinzu. Führen Sie diesen Befehl aus, um Parameter aus einer Zuordnung oder einem Arbeitsablauf hinzuzufügen, der als Anwendung bereitgestellt wurde.

Der infacmd das AddParameterSetEntries-Befehl verwendet die folgende Syntax:

```
AddParameterSetEntries

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application

<-parameterSetName|-ps> parameter set name

<-projectScope|-prs> path to the mapping or workflow that contains the parameters. For a
mapping, M1, in project P1 and folder F1, the path is P1/F1/mapping/M1.
```

<-paramNameValues|-pnv> parameter name-value pairs, separated by space

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis AddParameterSetEntries“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application	Erforderlich. Name der Anwendung, die den Parametersatz enthält.
parametersetname -ps	parameterset name	Erforderlich. Name des Parametersatzes.
-projectScope -prs	project scope	Erforderlich. Pfad der Zuordnung oder des Arbeitsablaufs, der die Parameter enthält. Für die Zuordnung M1 in Projekt P1 und Ordner F1 lautet der Pfad: P1/F1/Zuordnung/M1.
-paramNames -pnv	parameter names	Erforderlich. Namen-Wert-Paare des Parameters getrennt durch Leerzeichen. Setzen Sie Namen-Wert-Paare in doppelte Anführungszeichen. Versehen Sie jeden Wert mit einfachen Anführungszeichen. Verwenden Sie folgende Syntax: "parm1='valueA' " "parm2='valueB' " "parm3='valueC' ". Sie können Leerzeichen in einem Parameterwert verwenden. Sie können ein Apostroph (') oder einen Doppelpunkt (:) im Wert verwenden, wenn Sie für diese Zeichen einen umgekehrten Schrägstrich (\) als Escape-Zeichen verwenden. 'C:\Verzeichnis'

## BackupApplication

Sichert eine bereitgestellte Anwendung aus einem Datenintegrationsdienst in einer XML-Datei.

Die Backup-Datei enthält alle Eigenschafteneinstellungen für die Anwendung. Sie können die Anwendung in einem anderen Datenintegrationsdienst wiederherstellen. Sie müssen die Anwendung beenden, bevor Sie sie sichern.

Der Befehl „infacmd dis BackupApplication“ verwendet die folgende Syntax:

```
BackupApplication
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

<-Application|-a> application

<-FileName|-f> file\_name

In der folgenden Tabelle werden Optionen und Argumente für „infacmd dis BackupApplication“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domännennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domännennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomännennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-Application -a	anwendung	Erforderlich. Name der zu sichernden Anwendung.
Filename -f	file_name	Erforderlich. Name und Dateipfad der Backup-Datei für die Anwendung.

## CancelDataObjectCacheRefresh

Stoppt die letzte Anfrage zum Aktualisieren des logischen Datenobjekt-Cache. Wenn das Cache-Mapping ausgeführt wird, stoppt der Befehl die aktuelle Anfrage, um den logischen Datenobjekt-Cache zu aktualisieren. Zukünftige periodische Anfragen zum Aktualisieren des logischen Datenobjekt-Cache sind davon nicht betroffen.

Der Befehl „infacmd dis CancelDataObjectCacheRefresh“ verwendet die folgende Syntax:

```
CancelDataObjectCacheRefresh
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Application|-a> application
<-Folder|-f> folder
<-DataObject|-do> data_model.data_object
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd dis CancelDataObjectCacheRefresh“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie den Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdienst.
Application -a	application	Erforderlich. Name der Anwendung.
-Folder -f	folder	Ordner in der Anwendung, die das Datenobjekt enthält.
-DataObject -do	data_model.data_object	Erforderlich. Name des logischen Datenobjekts. Der Name muss die folgende Syntax aufweisen:  <data_model>.<data_object>

## CreateService

Erstellt einen Datenintegrationsdienst. Der Datenintegrationsdienst wird standardmäßig aktiviert, wenn Sie ihn erstellen.

Der Befehl „infacmd dis CreateService“ verwendet die folgende Syntax:

```
CreateService
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name | <-GridName|-gn> grid_name
[<-BackupNodes|-bn> node_name1,node_name2,...]
<-RepositoryService|-rs> model_repository_service_name
<-RepositoryUserName|-rsun> model_repository_user_name
<-RepositoryPassword|-rspd> model_repository_password
[<-RepositorySecurityDomain|-rssdn> model_repository_security_domain]
[<-HttpPort> http_port]
[<-HttpsPort> https_port]
[<-KeystoreFile|-kf> keystore_file_location]
[<-KeystorePassword|-kp> keystore_password]
[<-httpProtocolType|-pt> http_protocol_type]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis CreateService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdienst. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codeseite des verbundenen Repositorys kompatibel sein. Der Name darf nicht länger als 230 Zeichen sein und keine Leerzeichen, Wagenrückläufe, Tabulatoren oder die folgenden Zeichen enthalten:  / * ? < > "
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.



Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-NodeName -nn	node_name	Erforderlich, wenn Sie den Gitternamen nicht angeben. Knoten, auf dem der Datenintegrationsdienst ausgeführt wird. Sie können den Datenintegrationsdienst auf einem Knoten oder Gitter ausführen.
-GridName -gn	grid_name	Erforderlich, wenn Sie den Knotennamen nicht angeben. Gitter, in dem der Datenintegrationsdienst ausgeführt wird. Sie können den Datenintegrationsdienst auf einem Knoten oder Gitter ausführen.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Sicherungsknoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.
-RepositoryService -rs	model_repository_service_name	Modellrepository-Dienst, der Laufzeit-Metadaten speichert, die zur Ausführung der Mappings und SQL-Datendienste erforderlich sind.
-RepositoryUserName -rsun	model_repository_user_name	Benutzername zum Zugriff auf den Modellrepository-Dienst.
-RepositoryPassword -rspd	model_repository_password	Benutzerpasswort zum Zugriff auf den Modellrepository-Dienst.
-RepositorySecurityDomain -rssdn	model_repository_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer des Modellrepository gehört.
-HttpPort	http_port	Erforderlich, wenn Sie keinen HTTPS-Port angeben. Eindeutige HTTP-Portnummer, die für jeden Datenintegrationsdienst-Prozess verwendet wird. Nachdem Sie den Dienst erstellt haben, können Sie unterschiedliche Portnummern für jeden Datenintegrationsdienst-Prozess definieren. Der Standardwert ist 8095.
-HttpsPort	https_port	Erforderlich, wenn Sie keinen HTTP-Port angeben. Eindeutige HTTPS-Portnummer wird für jeden Datenintegrationsdienst-Prozess verwendet. Nachdem Sie den Dienst erstellt haben, können Sie unterschiedliche Portnummern für jeden Datenintegrationsdienst-Prozess definieren.

Option	Argument	Beschreibung
-KeystoreFile -kf	keystore_file_location	<p>Pfad und Dateiname der Schlüsselspeicherdatei, die die Schlüssel und Zertifikate enthält, die zur Verwendung des HTTPS-Protokolls für den Datenintegrationsdienst erforderlich sind. Sie können eine Schlüsselspeicherdatei mit einem Keytool erstellen. Keytool ist ein Dienstprogramm, das private oder öffentliche Schlüsselpaare und verknüpfte Zertifikate in einer Schlüsselspeicherdatei generiert und speichert. Sie können das selbstsignierte Zertifikat oder ein von einer Zertifizierungsbehörde signiertes Zertifikat verwenden.</p> <p>Wenn Sie den Datenintegrationsdienst auf einem Gitter ausführen, muss die Schlüsselspeicherdatei auf jedem Knoten im Gitter die gleichen Schlüssel enthalten.</p>
-KeystorePassword -kp	keystore_password	Passwort für die Schlüsselspeicherdatei.
-httpProtocolType -pt	http_protocol_type	<p>Sicherheitsprotokoll, das vom Datenintegrationsdienst verwendet wird. Geben Sie einen der folgenden Werte ein:</p> <ul style="list-style-type: none"> <li>- HTTP. Anfragen an den Dienst müssen eine HTTP-URL verwenden.</li> <li>- HTTPS. Anfragen an den Dienst müssen eine HTTPS-URL verwenden.</li> <li>- Both. Anfragen an den Dienst, die entweder eine HTTP- oder eine HTTPS-URL verwenden können.</li> </ul> <p>Wenn Sie den HTTP-Protokolltyp auf HTTPS oder Both einstellen, aktivieren Sie TLS (Transport Layer Security) für den Dienst.</p> <p>Sie können TLS auch für jeden Webdienst aktivieren, der einer Anwendung bereitgestellt ist. Wenn Sie HTTPS für den Data Integration Service und TLS für den Webdienst aktivieren, verwendet der Webdienst eine HTTPS-URL. Wenn Sie HTTPS für den Data Integration Service und nicht für den Webdienst aktivieren, kann der Webdienst eine HTTP-URL oder eine HTTPS-URL nutzen. Wenn Sie TLS für einen Webdienst aktivieren, aber HTTPS nicht für den Data Integration Service aktivieren, startet der Webdienst nicht.</p> <p>Der Standardwert ist HTTP.</p>

## compareMapping

Vergleicht zwei abgefragte Zuordnungen.

Fragen Sie die Objekte ab, um Eigenschaften, Umwandlungseigenschaften und Ports innerhalb von Umwandlungen zu vergleichen.

Geben Sie zum Abfragen von Entwurfszeitobjekten das Entwurfszeit-Modellrepository an. Geben Sie zum Abfragen von Laufzeitobjekten kein Modellrepository an. Die Abfrage verwendet das Modellrepository, das mit dem Datenintegrationsdienst verknüpft ist, der die Abfrage ausführt.

**Hinweis auf veraltete Version:** Ab Version 10.5 ist der Befehl „infacmd dis compareMapping“ veraltet und wird in einer zukünftigen Version entfernt. Wenn Sie Skripts verwenden, die auf „infacmd dis compareMapping“ basieren, empfiehlt Informatica, die Skripts mit dem neuen Befehl „infacmd dis

compareObject“ zu aktualisieren. Veraltete Funktionen werden unterstützt. Informatica beabsichtigt jedoch, die Unterstützung in einer zukünftigen Version einzustellen. Informatica empfiehlt, dass Sie auf andere Funktionen umstellen, bevor die Unterstützung für die jeweilige Funktion eingestellt wird.

Der Befehl „infacmd dis compareMapping“ verwendet die folgende Syntax:

```
compareMapping

<-DomainName|-dn> domain_name

<-ServiceName|-sn> DIS_service_name

<-UserName|-un> DIS_user_name

<-Password|-pd> DIS_password

[<-SecurityDomain|-sdn> DIS_security_domain]

[<-sourceRepositoryService|-srcrs> source_MRS_name]

[<-sourceRepositoryUserName|-srcrsun> source_MRS_user_name]

[<-sourceRepositoryPassword|-srcrspd> source_MRS_password]

[<-sourceRepositorySecurityDomain|-srcrssdn> source_MRS_security_domain]

<-sourceQuery|-srcq> source_query

[<-targetRepositoryService|-tgtrs> target_MRS_name]

[<-targetRepositoryUserName|-tgtrsun> target_MRS_user_name]

[<-targetRepositoryPassword|-tgtrspd> target_MRS_password]

[<-targetRepositorySecurityDomain|-tgtrssdn> target_MRS_security_domain]

<-targetQuery|-tgtq> target_query

[<-TimeZone|-tz> time_zone]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis compareMapping“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	DIS-Dienstname	Erforderlich. Name des Datenintegrationsdiensts.

Option	Argument	Beschreibung
-UserName -un	DIS-Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	DIS-Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/ Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	DIS-Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.
-sourceRepositoryService -srcrs	MRS-Quell-Benutzername	Optional. Name des Modellrepository-Diensts für das Quellobjekt.
-sourceRepositoryUserName -srcrsun	MRS-Quell-Benutzername	Optional. Der Benutzername für den Modellrepository-Dienst, der für den Zugriff auf das Quellobjekt verwendet wird. Sie können den Benutzernamen mit der Option -srcrsun oder der Umgebungsvariablen INFA_SOURCE_REPOSITORY_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -srcrsun Vorrang.

Option	Argument	Beschreibung
-sourceRepositoryPassword -srcrspd	MRS-Quellpasswort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -srcrspd oder der Umgebungsvariablen INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-srcrspd“ festgelegte Passwort Vorrang.
-sourceRepositorySecurityDomain -srcrstdn	MRS-Quell-Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -srcrstdn oder der Umgebungsvariablen INFA_DEFAULT_SOURCE_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänenennamen mit beiden Methoden festlegen, hat die Option -srcrstdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.
-sourceQuery -srcq	Quellabfrage	Erforderlich. Eine Zeichenfolge, die das Quellobjekt abfragt. Weitere Informationen hierzu finden Sie unter <a href="#">“Abfragen” auf Seite 290</a> .
-targetRepositoryService -tgtrs	MRS-Ziel-Name	Optional. Name des Modellrepository-Diensts für das Zielobjekt.
-targetRepositoryUserName -tgtrsun	MRS-Ziel-Benutzername	Optional. Der Benutzername für den Modellrepository-Dienst, der für den Zugriff auf das Zielobjekt verwendet wird. Sie können den Benutzernamen mit der Option -tgtrsun oder der Umgebungsvariablen INFA_TARGET_REPOSITORY_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -tgtrsun Vorrang.
-targetRepositoryPassword -tgtrspd	MRS-Ziel-Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -tgtrspd oder der Umgebungsvariablen INFA_TARGET_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-tgtrspd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-targetRepositorySecurityDomain -tgtssdn	MRS-Ziel-Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -tgtssdn oder der Umgebungsvariablen INFA_DEFAULT_TARGET_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -tgtssdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.
-targetQuery -tgtq	Zielabfrage	Erforderlich. Eine Zeichenfolge, die das Zielobjekt abfragt. Weitere Informationen hierzu finden Sie unter <a href="#">“Abfragen” auf Seite 290</a> .
-TimeZone -tz	Zeitzone	Optional. Standardmäßig verwendet der Befehl die Zeitzone auf dem Computer, auf dem der Datenintegrationsdienstprozess ausgeführt wird. Eine Liste der gültigen Zeitzeonen finden Sie in der Klasse „java.time.ZoneID“.

## compareObject

Vergleicht zwei abgefragte Objekte.

Fragen Sie die Objekte ab, um Objekteigenschaften, Umwandlungseigenschaften und Ports innerhalb von Umwandlungen zwischen dem Datenintegrationsdienst und dem Modellrepository-Dienst zu vergleichen. Sie können Objekte auf folgende Arten vergleichen:

- Entwurfszeit mit Entwurfszeit innerhalb einer Domäne
- Entwurfszeit mit Laufzeit innerhalb einer Domäne
- Laufzeit mit Laufzeit innerhalb einer Domäne
- Entwurfszeit mit Entwurfszeit über Domänen hinweg
- Laufzeit mit Laufzeit über Domänen hinweg

Geben Sie zum Abfragen von Entwurfszeitobjekten den Modellrepository-Dienst an. Geben Sie zum Abfragen von Laufzeitobjekten einen Datenintegrationsdienst an. Wenn Sie keinen Dienst angeben, wird die Abfrage über die API anhand von Laufzeitobjekten für den Datenintegrationsdienst ausgeführt, der die API hostet.

Der Befehl „infacmd dis compareObject“ verwendet die folgende Syntax:

```
compareObject
```

```

<-DomainName|-dn> domain_name

<-ServiceName|-sn> DIS_service_name

<-UserName|-un> DIS_user_name

<-Password|-pd> DIS_password

[<-SecurityDomain|-sdn> DIS_security_domain]

[<-sourceDomainName|-srcdn> source_domain_name]

[<-sourceRepositoryService|-srcrs> source_MRS_name]

[<-sourceDataIntegrationService|-srcdis> source_DIS_name]

[<-sourceRepositoryUserName|-srcrsun> source_MRS_user_name]

[<-sourceRepositoryPassword|-srcrspd> source_MRS_password]

[<-sourceRepositorySecurityDomain|-srcrssdn> source_MRS_security_domain]

<-sourceQuery|-srcq> source_query

[<-targetDomainName|-tgttn> target_domain_name]

[<-targetRepositoryService|-tgtrs> target_MRS_name]

[<-targetDataIntegrationService|-tgtdis> target_DIS_name]

[<-targetRepositoryUserName|-tgtrsun> target_MRS_user_name]

[<-targetRepositoryPassword|-tgtrspd> target_MRS_password]

[<-targetRepositorySecurityDomain|-tgtrssdn> target_MRS_security_domain]

<-targetQuery|-tgtq> target_query

[<-TimeZone|-tz> time_zone]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis compareMapping“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	DIS-Dienstname	Erforderlich. Name des Datenintegrationsdiensts.
-UserName -un	DIS-Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.

Option	Argument	Beschreibung
-Password -pd	DIS-Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/ Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	DIS-Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.
-sourceDomainName -srcdn	source_domain_name	Erforderlich. Name der Domäne für das Quellobjekt.
-sourceRepositoryService -srcrs	MRS-Quell-Benutzername	Optional. Name des Modellrepository-Diensts für das Quellobjekt.
-sourceDataIntegrationService -srcdis	source_DIS_name	Optional. Name des Datenintegrationsdiensts für das Quellobjekt.
-sourceRepositoryUserName -srcrsun	MRS-Quell-Benutzername	Optional. Der Benutzername für den Modellrepository-Dienst, der für den Zugriff auf das Quellobjekt verwendet wird. Sie können den Benutzernamen mit der Option -srcrsun oder der Umgebungsvariablen INFA_SOURCE_REPOSITORY_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -srcrsun Vorrang.
-sourceRepositoryPassword -srcrspd	MRS-Quellpasswort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/ Kleinschreibung beachtet. Sie können ein Passwort mit der Option -srcrspd oder der Umgebungsvariablen INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-srcrspd“ festgelegte Passwort Vorrang.



Option	Argument	Beschreibung
- sourceRepositorySecurityDomain -srcssdn	MRS-Quell-Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -srcssdn oder der Umgebungsvariablen INFA_DEFAULT_SOURCE_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -srcssdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.
-sourceQuery -srcq	Quellabfrage	Erforderlich. Eine Zeichenfolge, die das Quellobjekt abfragt. Weitere Informationen finden Sie unter <a href="#">"Abfragen" auf Seite 290</a> .
-targetDomainName -tgtdn	target_domain_name	Erforderlich. Name der Domäne für das Zielobjekt.
-targetRepositoryService -tgtrs	MRS-Ziel-Name	Optional. Name des Modellrepository-Diensts für das Zielobjekt.
-targetDataIntegrationService -tgtdis	target_DIS_name	Optional. Name des Datenintegrationsdiensts für das Zielobjekt.
-targetRepositoryUserName -tgtrsun	MRS-Ziel-Benutzername	Optional. Der Benutzername für den Modellrepository-Dienst, der für den Zugriff auf das Zielobjekt verwendet wird. Sie können den Benutzernamen mit der Option -tgtrsun oder der Umgebungsvariablen INFA_TARGET_REPOSITORY_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -tgtrsun Vorrang.
-targetRepositoryPassword -tgtrspd	MRS-Ziel-Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -tgtrspd oder der Umgebungsvariablen INFA_TARGET_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-tgtrspd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-targetRepositorySecurityDomain -tgtssdn	MRS-Ziel-Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -tgtssdn oder der Umgebungsvariablen INFA_DEFAULT_TARGET_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -tgtssdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.
-targetQuery -tgtq	Zielabfrage	Erforderlich. Eine Zeichenfolge, die das Zielobjekt abfragt. Weitere Informationen finden Sie unter <a href="#">"Abfragen" auf Seite 290</a>
-TimeZone -tz	Zeitzone	Optional. Standardmäßig verwendet der Befehl die Zeitzone auf dem Computer, auf dem der Datenintegrationsdienstprozess ausgeführt wird. Eine Liste der gültigen Zeitzonen finden Sie in der Klasse „java.time.ZoneID“.

## DeleteParameterSetEntries

Löscht Einträge aus einem Parametersatz. Führen Sie diesen Befehl aus, um Parametersatzeinträge für eine Zuordnung oder einen Arbeitsablauf zu löschen, der als Anwendung bereitgestellt wurde. Sie können bestimmte oder alle Parametersatzeinträge löschen.

Wenn ein zu löschender Parameter nicht im Parametersatz vorhanden ist, gibt infacmd eine Warnmeldung zurück. Die Meldung gibt an, dass der Parameter nicht gelöscht wird, weil er nicht im Parametersatz vorhanden ist.

Der infacmd-Befehl `DeleteParameterSetEntries` verwendet die folgende Syntax:

```

DeleteParameterSetEntries

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```

<-Application|-a> application

<-parameterSetName|-ps> parameter set name

<-projectScope|-prs> path to the mapping or workflow that contains the parameters

<-paramNames|-pnv> parameter names to delete, separated by spaces. For a mapping, M1, in
project P1 and folder F1, the path is P1/F1/mapping/M1.

<-all|> Delete all the parameters in the project scope.

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd deleteParameterSetEntries“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application	Erforderlich. Name der Anwendung, die den Parametersatz enthält.
parametersetname -ps	parameterset name	Erforderlich. Name des Parametersatzes.
-projectScope -prs	project scope	Erforderlich. Pfad der Zuordnung oder des Arbeitsablaufs, der die Parameter enthält. Für die Zuordnung M1 in Projekt P1 und Ordner F1 lautet der Pfad: P1/F1/Zuordnung/M1.
-paramNames -pnv	parameter names	Erforderlich. Durch Leerzeichen getrennte Namen von Parametersätzen, die gelöscht werden sollen. Verwenden Sie zum Löschen aller Parameter statt dieser Option die Option -all.
-all	all	Löschen Sie alle Parameter im Parametersatz.

# deployObjectsToFile

Stellt die Entwurfszeitobjekte in einer Anwendungs-Patch-Archivdatei bereit.

Fragen Sie die Objekte ab, die Sie in die Anwendungs-Patch-Archivdatei packen möchten. Sie können die Datei zum Durchführen folgender Aufgaben verwenden:

- Erstmaliges Bereitstellen einer inkrementellen Anwendung für einen Datenintegrationsdienst mithilfe des infacmd dis-Befehls [“DeployApplication” auf Seite 181](#).
- Aktualisieren einer bereitgestellten inkrementellen Anwendung mithilfe des infacmd tools-Befehls [“patchApplication” auf Seite 1234](#).
- Erneutes Bereitstellen einer inkrementellen Anwendung mithilfe des infacmd dis-Befehls [“UpdateApplication” auf Seite 261](#).

**Hinweis:** Der „infacmd dis deployObjectsToFile“ erstellt eine Anwendungs-Patch-Archivdatei auf jedem Knoten in einem Gitter. Sie können sich die Knotendetails auch im Abfragebericht ansehen.

Der Befehl „infacmd dis deployObjectsToFile“ verwendet die folgende Syntax:

```
deployObjectsToFile
<-DomainName|-dn> domain_name
<-ServiceName|-sn> DIS_service_name
<-UserName|-un> DIS_user_name
<-Password|-pd> DIS_password
[<-SecurityDomain|-sdn> DIS_security_domain]
<-RepositoryService|-rs> MRS_service_name
<-RepositoryUserName|-rsun> MRS_user_name
<-RepositoryPassword|-rspd> MRS_password
[<-RepositorySecurityDomain|-rssdn> MRS_security_domain]
<-Query|-q> Query
[<-TimeZone|-tz> time_zone]
<-PatchName|-ptn> patch_name
[<-PatchDescription|-ptd> patch_description]
<-Application|-a> application_name
[<-FilePath|-fp> DIS_file_path]
[<-OperatingSystemProfile|-osp> OSProfile_name]
[<-OverwriteDeployedFile|-ow> True | False]
[<-MappingDeploymentProperties|-mdp>
Mapping_Deployment_Property_key=value_pairs_separated_by_semicolon]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis deployObjectsToFile“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	DIS-Dienstname	Erforderlich. Name des Datenintegrationsdiensts.
-UserName -un	DIS-Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	DIS-Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	DIS-Sicherheitsdomäne	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.</p>
-RepositoryService -rs	MRS-Dienstname	Erforderlich. Name des Modellrepository-Diensts.
-RepositoryUserName -rsun	MRS-Benutzername	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -rsun oder der Umgebungsvariablen INFA_REPOSITORY_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -rsun Vorrang.</p>
-RepositoryPassword -rspd	MRS-Passwort	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -rspd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-rspd“ festgelegte Passwort Vorrang.</p>

Option	Argument	Beschreibung
- RepositorySecurityDomain -rssdn	MRS-Sicherheitsdomäne	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -rssdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -rssdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.</p>
-Query -q	query	Erforderlich. Eine Zeichenfolge, die das Objekt abfragt. Weitere Informationen hierzu finden Sie unter <a href="#">"Abfragen" auf Seite 290</a> .
-TimeZone -tz	Zeitzone	Optional. Standardmäßig verwendet der Befehl die Zeitzone auf dem Computer, auf dem der Datenintegrationsdienstprozess ausgeführt wird. Eine Liste der gültigen Zeitzonen finden Sie in der Klasse „java.time.ZoneID“.
-PatchName -ptn	Patch-Name:	Erforderlich. Name des Patches.
-PatchDescription -ptd	Patch-Beschreibung	Beschreibung des Patches.
-Application -a	application_name	Erforderlich. Name der inkrementellen Anwendung, die mit dem Patch aktualisiert werden soll.
-FilePath -fp	DIS-Dateipfad	Optional. Pfad der Anwendungs-Patch-Archivdatei auf dem Computer des Datenintegrationsdiensts. Sie können einen absoluten oder einen relativen Pfad zu der Datei angeben.



Option	Argument	Beschreibung
- OperatingSystemProfile -osp	OSProfile_name	Optional. Name des Betriebssystemprofils. Der Name des Betriebssystemprofils kann bis zu 80 Zeichen enthalten. Er darf weder Leerzeichen noch die folgenden Sonderzeichen enthalten:  % * + \ / ? ; < >
- OverwriteDeployedFile -ow	True False	Optional. Legen Sie die Option auf „True“ fest, um eine vorhandene Exportdatei zu überschreiben. Wenn eine Exportdatei vorhanden und diese Option auf FALSE festgelegt ist, schlägt der Export fehl. Der Standardwert ist „false“.
- MappingDeploymentProperties -mdp	Eigenschaftsschlüssel_der_Zuordnungsbereitstellung= Wertpaare_getrennt_durch_Semikolon	Optional. Legen Sie die Bereitstellungseigenschaften für die Zuordnung fest, wie z. B. Optimierungsgrad, hohe Genauigkeit und Sortierreihenfolge.

## DeployApplication

Stellt einem Datenintegrationsdienst eine Anwendung bereit.

Der Befehl „infacmd dis DeployApplication“ verwendet die folgende Syntax:

```
DeployApplication
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-FileName|-f> file_name
<-Application|-a> application
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis DeployApplication“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
Filename -f	file_name	Erforderlich. Name der Anwendungsdatei.
-Application -a	application	Erforderlich. Name der bereitzustellenden Anwendung. Im Fall eines Namenskonflikts schlägt die Bereitstellung fehl.

## disableMappingValidationEnvironment

Deaktiviert die ausgewählte Validierungsumgebung für Zuordnungen, die im Datenintegrationsdienst bereitgestellt werden.

Verwenden Sie den ValidationEnvironment-Parameter, um eine Validierungsumgebung für ein Mapping zu deaktivieren. Wiederholen Sie den Befehl für jede Umgebung, die Sie entfernen möchten.

Verwenden Sie Filter, um ein oder mehrere Mappings in einer Anwendung anzugeben. Wenn Sie keine Filter einschließen, aktualisiert der Befehl alle Mappings, die im Datenintegrationsdienst bereitgestellt werden. Damit ein Mapping geändert werden kann, muss es allen festgelegten Filtern entsprechen.

Änderungen werden wirksam, nachdem Sie den Datenintegrationsdienst wiederverwendet haben.

Der Befehl infacmd dis disableMappingValidationEnvironment verwendet die folgende Syntax:

```
disableMappingValidationEnvironment
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-Application|-a> application_name]
[<-ProjectName|-pn> project_name]
[<-MappingNamesFilter|-mnf> mapping_names]
[<-ExecutionEnvironmentFilter|-eef> execution_environment_name]
[<-ExecutionEnvironmentParameterNameFilter|-pnf> parameter_name]
[<-ExecutionEnvironmentParameterDefaultValueFilter|-pdvf> parameter default value]
<-ValidationEnvironment|-ve> validation_environment_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente von disableMappingValidationEnvironment beschrieben:

Option	Argument	Beschreibung
DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>

Option	Argument	Beschreibung
UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
Passwort -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts.
Anwendung -a	application_name	Optional. Name der Anwendung, die eine oder mehrere Zuordnungen enthält. Wenn Sie die Anwendung nicht angeben, aktualisiert der Befehl alle Anwendungen, die im Datenintegrationsdienst bereitgestellt werden.
-ProjectName -pn	project_name	Optional. Name des Projekts, das die Zuordnung enthält. Wenn Sie keinen Projektnamen angeben, aktualisiert der Befehl alle Projekte im Modellrepository.

Option	Argument	Beschreibung
MappingNamesFilter -mnf	mapping_names	Optional. Die Namen der Mappings, für die Sie die Validierungsumgebung deaktivieren möchten. Trennen Sie die Namen der Mappings durch Kommas. Standardmäßig werden alle Mappings berücksichtigt, die für den Datenintegrationsdienst bereitgestellt werden.
ExecutionEnvironmentFilter -eef	execution_environment_name	Optional. Geben Sie die Ausführungsumgebung für die zu entfernende Validierungsumgebung an. Sie können entweder „Nativ“, „Hadoop“ oder „Databricks“ eingeben. Standardmäßig wird die Validierungsumgebung für alle Engines auf Basis anderer Filterkriterien geändert.
ValidationEnvironment -ve	validation_environment_name	Erforderlich. Name der Validierungsumgebung, die aus einem Mapping entfernt werden soll. Sie können einen der folgenden Werte eingeben: <ul style="list-style-type: none"> <li>- native</li> <li>- blaze</li> <li>- spark</li> <li>- spark-databricks</li> </ul> Führen Sie den Befehl für jede zu entfernende Validierungsumgebung aus.
ExecutionEnvironmentParameterNameFilter -pnf	name_of_parameter	Optional. Wählt nur Zuordnungen aus, deren Parametername mit diesem Wert übereinstimmt.  Beispiel: infacmd.sh mrs enableValidationEnvironment -pnf MyParam -ve Databricks

Option	Argument	Beschreibung
ExecutionEnvironmentParameterDefaultValueFilter -pdvf	parameter_default_value	Optional. Wählt nur Zuordnungen aus, deren standardmäßiger Parametername mit diesem Wert übereinstimmt.  Beispiel: infacmd.sh mrs enableValidationEnvironment -pdvf Hadoop -ve Databricks
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

## enableMappingValidationEnvironment

Aktiviert eine Validierungsumgebung für Zuordnungen, die im Datenintegrationsdienst bereitgestellt werden. In den Eigenschaften der Validierungsumgebung für Zuordnungen werden die Engines angegeben, auf denen die Zuordnung zur Ausführung validiert wird.

Verwenden Sie den Parameter „ValidationEnvironment“ zur Angabe einer Validierungsumgebung. Wiederholen Sie den Befehl und geben Sie eine andere Validierungsumgebung an, um eine zusätzliche Validierungsumgebung für das Mapping zu aktivieren.

Verwenden Sie Filter, um ein oder mehrere Mappings in einer Anwendung oder in allen Anwendungen anzugeben, die für einen Datenintegrationsdienst bereitgestellt werden. Wenn Sie keine Filter einschließen, aktualisiert der Befehl alle Mappings, die im Datenintegrationsdienst bereitgestellt werden. Damit ein Mapping geändert werden kann, muss es allen festgelegten Filtern entsprechen.

Änderungen werden wirksam, nachdem Sie den Datenintegrationsdienst wiederverwendet haben.

Der Befehl infacmd dis enableMappingValidationEnvironment verwendet die folgende Syntax:

```
enableMappingValidationEnvironment
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-Application|-a> application_name]
[<-ConnectionName|-cn> connection_name]
[<-ProjectName|-pn> project_name]
[<-MappingNamesFilter|-mnf> mapping_names]
[<-ExecutionEnvironmentFilter|-eef> execution_environment_name]
[<-ExecutionEnvironmentParameterNameFilter|-pnf> parameter_name]
[<-ExecutionEnvironmentParameterDefaultValueFilter|-pdvf> parameter default value]
<-ValidationEnvironment|-ve> validation_environment_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente von enableMappingValidationEnvironment beschrieben:

Option	Argument	Beschreibung
DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>



Option	Argument	Beschreibung
UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
Passwort -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts.
Anwendung -a	application_name	Optional. Name der Anwendung, die eine oder mehrere Zuordnungen enthält. Wenn Sie die Anwendung nicht angeben, aktualisiert der Befehl alle Anwendungen, die im Datenintegrationsdienst bereitgestellt werden.
-ProjectName -pn	project_name	Optional. Name des Projekts, das die Zuordnung enthält. Wenn Sie keinen Projektnamen angeben, aktualisiert der Befehl alle Projekte im Modellrepository.

Option	Argument	Beschreibung
ConnectionName -cn	connection_name	<p>Name der Verbindung für die zu verwendende Validierungsumgebung der Zuordnung. Die Verbindung überschreibt eine vorhandene Verbindung oder einen Verbindungsparameter, der für die Umgebung festgelegt wurde.</p> <p>Erforderlich, um die nicht-native Umgebung zu aktivieren, wenn in der angegebenen Zuordnung keine Verbindung vorhanden ist. Optional, um die native Umgebung zu aktivieren, oder wenn bereits eine Verbindung vorhanden ist.</p>
MappingNamesFilter -mnf	mapping_names	<p>Optional. Die Namen der Mappings, für die Sie die Validierungsumgebung aktivieren möchten. Trennen Sie die Namen der Mappings durch Kommas.</p> <p>Standardmäßig werden alle Mappings berücksichtigt, die für den Datenintegrationsdienst bereitgestellt werden.</p>
ExecutionEnvironmentFilter -eef	execution_environment_name	<p>Optional. Identifiziert die Ausführungsumgebung, nach der gefiltert werden soll. Sie können „Nativ“, „Hadoop“ oder „Databricks“ eingeben.</p> <p>Standardmäßig wird die Validierungsumgebung für alle Engines auf Basis anderer Filterkriterien geändert.</p>
ValidationEnvironment -ve	validation_environment_name	<p>Erforderlich. Name der Validierungsumgebung, die für ein Mapping aktiviert werden soll. Sie können einen der folgenden Werte eingeben:</p> <ul style="list-style-type: none"> <li>- native</li> <li>- blaze</li> <li>- spark</li> <li>- spark-databricks</li> </ul> <p>Führen Sie den Befehl für jede zu aktivierende Validierungsumgebung aus.</p>
ExecutionEnvironmentParameterNameFilter -pnf	name_of_parameter	<p>Optional. Wählt nur Zuordnungen aus, deren Parametername mit diesem Wert übereinstimmt.</p> <p>Beispiel: <code>infacmd.sh mrs enableValidationEnvironment -pnf MyParam -ve Databricks</code></p>

Option	Argument	Beschreibung
ExecutionEnvironmentParameterDefaultValueFilter -pdvf	parameter_default_value	Optional. Wählt nur Zuordnungen aus, deren standardmäßiger Parametername mit diesem Wert übereinstimmt.  Beispiel: infacmd.sh mrs enableValidationEnvironment -pdvf Hadoop -ve Databricks
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

## ListApplicationObjectPermissions

Listet die Berechtigungen auf, die einem Benutzer oder einer Gruppe für ein Anwendungsobjekt zugewiesen sind, wie z. B. eine Zuordnung oder ein Arbeitsablauf.

Der Befehl „infacmd dis ListApplicationObjectPermissions“ verwendet die folgende Syntax:

```
ListApplicationObjectPermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-ApplicationObjectType|-t> application_object_type_Mapping_Workflow
<-ApplicationObject|-ao> application_object_name
<<-Direct> direct_permission_only|<-Effective> effective_permission_only>
```

In der folgenden Tabelle werden die Optionen und Argumente für infacmd dis ListApplicationObjectPermissions beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domännennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domännennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomännennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-Application -a	application_name	Erforderlich. Name der Anwendung.
-ApplicationObjectType -t	application_object_type	Erforderlich. Typ des Anwendungsobjekttyps. Geben Sie einen der folgenden Werte ein: - Zuordnung - Arbeitsablauf
-ApplicationObject -ao	application_object_name	Erforderlich. Name des Anwendungsobjekts.
-Direct   -Effective	direct   effective	Erforderlich. Ebene der aufzulistenden Berechtigungen. Direkte Berechtigungen sind Berechtigungen, die dem Benutzer oder der Gruppe direkt zugewiesen werden. Effektive Berechtigungen umfassen direkte Berechtigungen und geerbte Berechtigungen.

## ListApplicationObjects

Listet die Objekte auf, die eine Anwendung enthält.

Wenn Sie die Option -ListObjectTypes verwenden, listet der Befehl auch den Typ jedes Objekts auf.

Der infacmd des ListApplicationObjects-Befehls verwendet die folgende Syntax:

```
ListApplicationObjects
[<-DomainName|-dn> domain_name]
[<-DomainAddress|-da> domain_address. syntax - host:port]
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
[<-ObjectType|-t> object_type]
[<-ListObjectType|-lt> list_object_type]
[<-PageSize|-ps> page_size]
[<-PageIndex|-pi> page_index]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd des ListApplicationObjects“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Optional. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-DomainAddress -da	domain_address	Optional. Adresse der Informatica-Domäne.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application	Erforderlich. Name der Anwendung.

Option	Argument	Beschreibung
-ObjectType -t	object_type	Optional. Typ des aufzulistenden Objekts. Sie können diese Option zum Filtern der Ergebnisse nach Objekttyp verwenden.
-ListObjectType -lt	true   false	Optional. Geben Sie einen der folgenden Werte ein: - True - Falsch
-PageSize -ps	page_size	Erforderlich, wenn Sie die Option „PageIndex“ angeben. Die Anzahl der anzuzeigenden Ergebnisse in jeder Gruppe. Wenn Sie eine Seitengröße angeben, verwalten Sie Befehlsergebnisse in Gruppen. Wenn Sie beispielsweise -PageSize 5 angeben, gibt der Befehl Ergebnisse in Fünfer- oder kleineren Gruppen zurück.
-PageIndex -pi	page_index	Optional. Beginnend mit null, die Anzahl der anzuzeigenden Seitenergebnisse. Wenn Sie beispielsweise -PageSize 5 -PageIndex 0 angeben, gibt der Befehl die erste Seite mit fünf Ergebnissen zurück, die Ergebnisse eins bis fünf.  Wenn Sie diese Option auslassen, gibt der Befehl die erste PageSize mit Ergebnissen zurück. Standardwert ist Null.

## ListApplicationOptions

Listet die Eigenschaften für eine Anwendung auf.

Der Befehl „infacmd dis ListApplicationOptions“ verwendet die folgende Syntax:

```
ListApplicationOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListApplicationOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.



Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	anwendung	Erforderlich. Name der Anwendung.

## ListApplicationPermissions

Listet alle Berechtigungen auf, die ein Benutzer bzw. eine Gruppe für eine Anwendung besitzt.

Der Befehl „infacmd dis ListApplicationPermissions“ verwendet die folgende Syntax:

```
ListApplicationPermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<<-Direct> direct_permission_only|<-Effective> effective_permission_only>
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListApplicationPermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-Application -a	application_name	Erforderlich. Name der Anwendung.
-Direct   -Effective	direct   effective	Erforderlich. Ebene der aufzulistenden Berechtigungen. Direkte Berechtigungen sind Berechtigungen, die dem Benutzer oder der Gruppe direkt zugewiesen werden. Effektive Berechtigungen umfassen direkte Berechtigungen und geerbte Berechtigungen.

# ListApplications

Listet die Anwendungen auf, die in einem Datenintegrationsdienst bereitgestellt werden.

Der Befehl „infacmd dis ListApplications“ verwendet die folgende Syntax:

```
ListApplications
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListApplications“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, für den Anwendungen aufgelistet werden sollen.

## ListComputeOptions

Listet Eigenschaften des Datenintegrationsdiensts für einen Knoten mit der Berechnungsrolle auf.

Der infacmd dis ListComputeOptions-Befehl verwendet die folgende Syntax:

```
ListComputeOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „dis ListComputeOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
NodeName -nn	node_name	Erforderlich. Knoten mit der Berechnungsrolle, die dem Datenintegrationsdienst oder dem Datenintegrationsdienstgitter zugewiesen ist.

## ListDataObjectOptions

Listet Eigenschaften eines Datenobjekts auf.

Der Befehl „infacmd dis ListDataObjectOptions“ verwendet die folgende Syntax:

```
ListDataObjectOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
<-Folder|-f> folder
<-DataObject|-do> data_model.data_object
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListDataObjectOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdienst.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	Passwort	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-Application -a	anwendung	Erforderlich. Name der Anwendung.

Option	Argument	Beschreibung
-Folder -f	folder	Erforderlich. Repository-Ordner, der das Datenobjekt enthält.
DataObject -do	data_model.data_object	Erforderlich. Name des Datenobjekts.

## ListMappingEngines

Listet die Ausführungs-Engines der in einem Datenintegrationsdienst bereitgestellten Zuordnungen auf. Sie können die Ergebnisse nach Anwendung, Validierungsumgebung, Ausführungsumgebung sowie nach Parametern für die Ausführungsumgebung filtern. Wenn Sie keine Filter angeben, listet der Befehl die Ausführungs-Engines aller bereitgestellten Zuordnungen auf.

Der Befehl „infacmd dis listMappingEngines“ verwendet die folgende Syntax:

```
ListMappingEngines
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-ProjectName|-pn> project_name]
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-Application|-a> application_name]
[<-ValidationEnvironmentFilter|-vef> validation_environment_name]
[<-ExecutionEnvironmentFilter|-eef> execution_environment_name]
[<-ExecutionEnvironmentParamNameFilter|-pnf> execution_environment_parameter_name]
```



In der folgenden Tabelle werden die Optionen und Argumente für infacmd dis listMappingEngines beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ProjectName -pn	project_name	Optional. Name des Projekts, das die Zuordnung enthält. Wenn Sie keinen Projektnamen angeben, aktualisiert der Befehl alle Projekte im Modellrepository.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
Anwendung -a	application_name	<p>Optional. Filtert die Zuordnungen nach der bereitgestellten Anwendung, die die Zuordnungen enthält. Geben Sie den Namen der bereitgestellten Anwendung ein.</p>
ValidationEnvironmentFilter -vef	validation_environment_name	<p>Optional. Filtert die Zuordnungen nach der Validierungsumgebung, in der die Zuordnungsdefinition validiert wird. Sie können einen der folgenden Werte eingeben:</p> <ul style="list-style-type: none"> <li>- native</li> <li>- blaze</li> <li>- spark</li> <li>- spark-databricks</li> </ul>

Option	Argument	Beschreibung
ExecutionEnvironmentFilter -eef	execution_environment_name	Optional. Filtert die Zuordnungen nach der Ausführungsumgebung, in der die Zuordnungen ausgeführt werden. Sie können „Nativ“, „Hadoop“ oder „Databricks“ eingeben.
ExecutionEnvironmentParamNameFilter -pnf	execution_environment_parameter_name	Optional. Filtert die Zuordnungen nach dem Parameter Ausführungsumgebung. Geben Sie den Namen des Parameters Ausführungsumgebung ein.

## ListParameterSetEntries

Listet die Einträge in einem Parametersatz auf.

Der infacmd dis ListParameterSetEntries-Befehl verwendet die folgende Syntax:

```
ListParameterSetEntries

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application

<-parameterSetName|-ps> parameter set name

<-projectScope|-prs> path to the mapping or workflow that contains the parameters. For a mapping, M1, in project P1 and folder F1, the path is P1/F1/mapping/M1.
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListParameterSetEntries“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-Application -a	application	<p>Erforderlich. Name der Anwendung, die den Parametersatz enthält.</p>

Option	Argument	Beschreibung
parametersetname - ps	parameterset name	Erforderlich. Name des Parametersatzes.
-projectScope -prs	project scope	Erforderlich. Pfad der Zuordnung oder des Arbeitsablaufs, der die Parameter enthält. Für die Zuordnung M1 in Projekt P1 und Ordner F1 lautet der Pfad: P1/F1/Zuordnung/M1.

## ListParameterSetObjects

Listet die Objekte in einem bestimmten Parametersatz auf.

Der infacmd-Befehl `dis ListParameterSetObjects` verwendet die folgende Syntax:

```
ListParameterSetObjects
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Password|-ps> parameter set
<-Application|-a> application that contains the parameter set
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd `dis ListParameterSetObjects`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-parameterset -ps	parameter set	<p>Erforderlich. Der Name des anzuzeigenden Parametersatzes.</p>
-Application -a	application	<p>Erforderlich. Name der Anwendung, die den Parametersatz enthält.</p>

# ListParameterSets

Listet die Parametersätze in einer Anwendung auf.

Der infacmd dis ListParameterSets-Befehl verwendet die folgende Syntax:

```
ListParameterSets  
  
<-DomainName|-dn> domain_name  
  
<-ServiceName|-sn> service_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-SecurityDomain|-sdn> security_domain]  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]  
  
<-Application|-a> application
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListParameterSets“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application	Erforderlich. Name der Anwendung, die die Parametersätze enthält.

## listPatchNames

Listet alle Patches auf, die auf eine inkrementelle Anwendung angewendet wurden.

Der Befehl „infacmd dis listPatchNames“ verwendet die folgende Syntax:

```
listPatchNames
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilientTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
```



In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis listPatchNames“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -dun oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -dun Vorrang.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -dpd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -dsdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.
ResilientTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariablen INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit diesen beiden Methoden festlegen, hat die Option -re Vorrang.
Anwendung -a	application_name	Erforderlich. Name der inkrementellen Anwendung.

# ListSequenceObjectProperties

Listet die Eigenschaften für ein Sequenzdatenobjekt auf.

Der Befehl „infacmd dis listsequenceobjectproperties“ verwendet die folgende Syntax:

```
ListSequenceObjectProperties
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
<-SequenceObjectPath|-sop> sequence_object_path
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListSequenceObjectProperties“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Integrationsdiensts.  Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf nicht länger als 230 Zeichen sein und keine voran- bzw. nachgestellten Leerzeichen, Wagenrückläufe, Tabulatoren oder folgende Zeichen enthalten: / * ? < > "
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-Application -a	application	Erforderlich. Name der Anwendung.
-SequenceObjectPath -sop	Sequenzobjekt-Pfad	<p>Erforderlich. Pfad zum Sequenzdatenobjekt. Der Pfad muss die folgenden Objekte in der angegebenen Reihenfolge enthalten, sofern zutreffend:</p> <ul style="list-style-type: none"> <li>- Projekt</li> <li>- Ordner</li> <li>- SQL-Datendienst oder Webdienst</li> <li>- Mapping</li> <li>- Sequenzgeneratorumwandlung</li> <li>- Sequenzdatenobjekt</li> </ul> <p>Befindet sich das Sequenzdatenobjekt in einem Mapping, SQL-Datendienst oder Webdienst, müssen Sie vor dem Mapping-, SQL-Datendienst- oder Webdienstnamen ein Präfix angeben. Verwenden Sie die folgenden Präfixe mit Optionen im Befehl:</p> <ul style="list-style-type: none"> <li>- Mapping:&lt;Mapping-Name&gt;</li> <li>- SQLDS:&lt;SQL-Datendienstname&gt;</li> <li>- WS:&lt;Webdienstname&gt;</li> </ul> <p>Trennen Sie die Optionen mit einem Schrägstrich (/). Beispiel:</p> <pre>&lt;Projektname&gt;/&lt;Ordner&gt;/SQLDS:&lt;SQL-Datendienstname&gt;/Mapping:&lt;virtuelle Tabellenzuordnung&gt;/&lt;Sequenzgenerator-Umwandlung&gt;/&lt;Sequenzdatenobjekt-Name&gt;</pre>

# ListSequenceObjects

Listet die für eine Anwendung bereitgestellten Sequenzdatenobjekte auf.

Der Befehl „infacmd dis ListSequenceObjects“ verwendet die folgende Syntax:

```
ListSequenceObjects
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListSequenceObjects“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Integrationsdiensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codeseite des verbundenen Repositorys kompatibel sein. Der Name darf nicht länger als 230 Zeichen sein und keine Leerzeichen, Wagenrückläufe, Tabulatoren oder die folgenden Zeichen enthalten: / * ? < > "
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	anwendung	Erforderlich. Name der Anwendung.

## ListServiceProcessOptions

Listet die Eigenschaften eines Datenintegrationsdienst-Prozesses auf.

Der Befehl „infacmd dis ListServiceProcessOptions“ verwendet die folgende Syntax:

```
ListServiceProcessOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListServiceProcessOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdienst.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienstprozess ausgeführt wird.

## PurgeDataObjectCache

Bereinigt den Cache für ein logisches Datenobjekt. Wenn Caching für logische Datenobjekte aktiviert ist, löscht dieser Befehl bis auf die letzte Cache-Ausführung den gesamten Cache für ein logisches Datenobjekt. Wenn die aktuelle Cache-Ausführung vor dem in der Eigenschaft für den Cache-Aktualisierungszeitraum festgelegten Datum liegt, wird der aktuelle Cache ebenfalls gelöscht. Wenn Caching für logische Datenobjekte nicht aktiviert ist, löscht dieser Befehl den gesamten Cache für das logische Datenobjekt.

Sie müssen die Anwendung für ein logisches Datenobjekt deaktivieren, bevor Sie den Cache für Datenobjekte löschen.

Der Befehl „infacmd dis PurgeDataObjectCache“ verwendet die folgende Syntax:

```
PurgeDataObjectCache
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Application|-a> application
<-Folder|-f> folder
<-DataObject|-do> data_model.data_object
[<-PurgeAll|-pa> true|false]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis PurgeDataObjectCache“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.



Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
Application -a	anwendung	Name der Anwendung, die das Datenobjekt enthält.
Folder -f	folder	Name des Ordners, der das Datenobjektmodell enthält.
DataObject -do	data_model.data_object	Name des Datenobjekts mit dem Cache, der bereinigt werden soll.
-PurgeAll -pa	true   false	Optional. Löscht den gesamten Cache für ein logisches Datenobjekt.

## PurgeResultSetCache

Bereinigt die Ergebnissatz-Caches für eine Anwendung. Sie können den Cache für eine Anwendung bereinigen, wenn Sie die vorhandenen Ergebnissatz-Caches für die SQL-Datendienste und die Webdienste in der Anwendung nicht benötigen.

Der Befehl „infacmd dis PurgeResultSetCache“ verwendet die folgende Syntax:

```
PurgeResultSetCache
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Application|-a> application
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis PurgeResultSetCache“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
Application -a	anwendung	Name der Anwendung, deren Ergebnissatz-Cache bereinigt werden soll.

## queryDesignTimeObjects

Fragt Entwurfszeitobjekte aus einem Modellrepository ab und gibt eine Liste der Objekte zurück.

Der Befehl „`infacmd dis queryDesignTimeObjects`“ verwendet die folgende Syntax:

```
queryDesignTimeObjects
<-DomainName|-dn> domain_name
<-ServiceName|-sn> DIS_service_name
<-UserName|-un> DIS_user_name
<-Password|-pd> DIS_password
[<-SecurityDomain|-sdn> DIS_security_domain]
<-RepositoryService|-rs> MRS_service_name
<-RepositoryUserName|-rsun> MRS_user_name
<-RepositoryPassword|-rspd> MRS_password
[<-RepositorySecurityDomain|-rssdn> MRS_security_domain]
<-Query|-q> Query
[<-TimeZone|-tz> time_zone]
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd dis queryDesignTimeObjects`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts.

Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -dsdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.
-RepositoryService -rs	MRS-Dienstname	Erforderlich. Name des Modellrepository-Diensts.
-RepositoryUserName -rsun	MRS-Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -rsun oder der Umgebungsvariablen INFA_REPOSITORY_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -rsun Vorrang.

Option	Argument	Beschreibung
-RepositoryPassword -rspd	MRS-Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -rspd oder der Umgebungsvariablen INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-rspd“ festgelegte Passwort Vorrang.
-RepositorySecurityDomain -rssdn	MRS-Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -rssdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -rssdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.
-Query -q	query	Erforderlich. Eine Zeichenfolge, die das Objekt abfragt. Weitere Informationen hierzu finden Sie unter <a href="#">“Abfragen” auf Seite 290</a> .
-TimeZone -tz	Zeitzone	Optional. Standardmäßig verwendet der Befehl die Zeitzone auf dem Computer, auf dem der Datenintegrationsdienstprozess ausgeführt wird. Eine Liste der gültigen Zeitzonen finden Sie in der Klasse „java.time.ZoneID“.

## queryRunTimeObjects

Fragt Laufzeitobjekte ab, die in einem Datenintegrationsdienst bereitgestellt werden, und gibt eine Liste der Objekte zurück.

Der Befehl „infacmd dis queryRunTimeObjects“ verwendet die folgende Syntax:

```
queryRunTimeObjects
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
```

<-Query|-q> query

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis queryRunTimeObjects“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -dun oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -dun Vorrang.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -dpd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -dsdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.
-Query -q	query	Erforderlich. Eine Zeichenfolge, die das Objekt abfragt. Weitere Informationen hierzu finden Sie unter <a href="#">“Abfragen” auf Seite 290</a> .

# RefreshDataObjectCache

Aktualisiert einen Datenobjekt-Cache.

Der Befehl „infacmd dis RefreshDataObjectCache“ verwendet die folgende Syntax:

```
RefreshDataObjectCache  
  
<-DomainName|-dn> domain_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-SecurityDomain|-sdn> security_domain]  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]  
  
<-ServiceName|-sn> service_name  
  
<-Application|-a> application  
  
<-Folder|-f> folder  
  
<-DataObject|-do> data_model.data_object
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis RefreshDataObjectCache“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, für den die Anwendungen aufgelistet werden sollen.
-Application -a	anwendung	Erforderlich. Name der Anwendung, die das Datenobjekt enthält.
-Folder -f	folder	Erforderlich. Name des Ordners, der das Datenobjekt enthält.
-DataObject -do	data_model.data_object	Erforderlich. Name des Datenobjekts mit einem zu aktualisierenden Cache.

## RenameApplication

Benennt eine bereitgestellte Anwendung um. Bevor Sie eine Anwendung umbenennen, führen Sie infacmd dis StopApplication aus, um die Anwendung zu beenden.

Der Befehl „infacmd dis RenameApplication“ verwendet die folgende Syntax:

```

RenameApplication
<-DomainName|-dn> domain_name
<-UserName|-un> user_name

```



```

<-Password|-pd> password

<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-Application|-a> application

<-NewName|-n> new_name

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis RenameApplication“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-Application -a	anwendung	Erforderlich. Name der aktuellen Anwendung.
-NewName -n	new_name	Erforderlich. Neuer Name für die Anwendung.

## replaceMappingHadoopRuntimeConnections

Ersetzt die Hadoop-Verbindung aller Mappings in bereitgestellten Anwendungen durch eine andere Hadoop-Verbindung. Der Datenintegrationsdienst verwendet die Hadoop-Verbindung zum Verbinden mit dem Hadoop-Cluster, um Mappings in der Hadoop-Umgebung auszuführen.

Der Befehl ändert keine Hadoop-Verbindungen in den Umwandlungen. Sie können den Namen der Anwendung angeben, um die Hadoop-Verbindung einer Anwendung zu ersetzen.

Der Befehl infacmd dis replaceMappingHadoopRuntimeConnections verwendet die folgende Syntax:

```
replaceMappingHadoopRuntimeConnections
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
```

```

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-ApplicationName|-an> application_name]

<-OldConnectionName|-oc> connection_name_of_old_connection_to_replace

<-NewConnectionName|-nc> connection_name_of_new_connection

```

In der folgenden Tabelle werden die Optionen und Argumente von `replaceMappingHadoopRuntimeConnections` beschrieben:

Option	Argument	Beschreibung
DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts.
UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
Passwort -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.</p>
ApplicationName -an	application_name	<p>Optional. Name der Anwendung, die das Mapping enthält. Wenn Sie diese Option angeben, ersetzt der Befehl die Hadoop-Verbindung nur für die Anwendung.</p>
OldConnectionName -oc	connection_name_of_old_connection_to_replace	<p>Erforderlich. Name der Hadoop-Verbindung, die Sie ersetzen möchten.</p>
NewConnectionName -nc	connection_name_of_new_connection	<p>Erforderlich. Name der Hadoop-Verbindung, die vom Datenintegrationsdienst verwendet werden muss, um eine Verbindung mit dem Hadoop-Cluster für die Ausführung von Mappings in Hadoop herzustellen.</p>

# RestoreApplication

Stellt eine Anwendung aus einer Backup-Datei wieder her. Wenn Sie eine wiederhergestellte Anwendung bereitstellen, richtet sich der Anwendungsstatus nach dem standardmäßigen Bereitstellungsmodus. Die Anwendungseigenschaften werden in der wiederhergestellten Anwendung beibehalten.

Der Befehl „infacmd dis RestoreApplication“ verwendet die folgende Syntax:

```
RestoreApplication  
  
<-DomainName|-dn> domain_name  
  
<-ServiceName|-sn> service_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-SecurityDomain|-sdn> security_domain]  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]  
  
<-FileName|-f> file_name  
  
[<-Application|-a> application]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis RestoreApplication“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdienst, in dem die Anwendung wiederhergestellt werden soll.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-FileName -f	file_name	Erforderlich. Name der Backup-Datei der Anwendung.
-Application -a	anwendung	Optional. Name der Anwendung nach deren Bereitstellung. Im Fall eines Namenskonflikts schlägt die Bereitstellung fehl.

## SetApplicationPermissions

Weist Berechtigungen für eine Anwendung einem Benutzer oder einer Gruppe zu oder verweigert diese.

Mit den Optionen -ap oder -dp des SetApplicationPermissions-Befehls können Sie Berechtigungen für Benutzer erteilen oder verweigern. Wenn Sie mit einer der Optionen Berechtigungen nicht explizit erteilen oder verweigern, werden alle Berechtigungen für die Anwendung widerrufen.

Der Befehl „infacmd dis SetApplicationPermissions“ verwendet die folgende Syntax:

```
SetApplicationPermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
```

```

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application_name

<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>

[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]

[<-AllowedPermissions|-ap> allowed_permissions]

[<-DeniedPermissions|-dp> denied_permissions]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis SetApplicationPermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung.
-GranteeUserName  GranteeGroupName -gun -ggn	grantee_user_name  grantee_group_name	Erforderlich. Benutzername bzw. Gruppenname, für den Berechtigungen festgelegt oder verweigert werden sollen.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, zu der der Benutzer gehört.
-AllowedPermissions -ap	allowed_permissions	<p>Optional. Liste der zulässigen Berechtigungen. Geben Sie eine der folgenden Berechtigungen durch Leerzeichen getrennt ein:</p> <ul style="list-style-type: none"> <li>- View. Benutzer können die Anwendung anzeigen.</li> <li>- Grant. Benutzer können Berechtigungen für die Anwendung gewähren und entziehen.</li> <li>- Execute. Benutzer können die Anwendung ausführen.</li> </ul>
-DeniedPermissions -dp	denied_permissions	<p>Optional. Liste der Berechtigungen, die Benutzern verweigert werden sollen. Trennen Sie jeden Parameter durch ein Leerzeichen. Geben Sie eine der folgenden Berechtigungen durch Leerzeichen getrennt ein:</p> <ul style="list-style-type: none"> <li>- View. Benutzer können die Anwendung anzeigen.</li> <li>- Grant. Benutzer können Berechtigungen für die Anwendung weder gewähren noch entziehen.</li> <li>- Execute. Benutzer können die Anwendung nicht ausführen.</li> </ul>



# SetApplicationObjectPermissions

Weist Berechtigungen für ein Anwendungsobjekt zu bzw. lehnt diese ab, wie z. B. ein Mapping oder Arbeitsablauf zu einem Benutzer bzw. einer Gruppe.

Mit den Optionen -ap oder -dp des SetApplicationObjectPermissions-Befehls können Sie Berechtigungen für Benutzer erteilen oder verweigern. Wenn Sie mit einer der Optionen Berechtigungen nicht explizit erteilen oder verweigern, erbt der Benutzer die Berechtigung auf Anwendungsebene für die Zuordnung oder den Arbeitsablauf.

Der Befehl „infacmd dis SetApplicationObjectPermissions“ verwendet die folgende Syntax:

```
SetApplicationObjectPermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-ApplicationObjectType|-t> application_object_type_Mapping_Workflow
<-ApplicationObject|-ao> application_object_name
<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>
[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]
[<-AllowedPermissions|-ap> allowed_permissions]
[<-DeniedPermissions|-dp> denied_permissions]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis SetApplicationObjectPermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-Application -a	application_name	Erforderlich. Name der Anwendung.
-ApplicationObjectType -t	application_object_type	<p>Erforderlich. Typ des Anwendungsobjekttyps. Geben Sie einen der folgenden Werte ein:</p> <ul style="list-style-type: none"> <li>- Zuordnung</li> <li>- Arbeitsablauf</li> </ul>

Option	Argument	Beschreibung
-ApplicationObject -ao	application_object_name	Erforderlich. Name des Anwendungsobjekts.
-GranteeUserName  GranteeGroupName -gun -ggn	grantee_user_name  grantee_group_name	Erforderlich. Benutzername bzw. Gruppenname, für den Berechtigungen festgelegt oder verweigert werden sollen.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, zu der der Benutzer gehört.
-AllowedPermissions -ap	allowed_permissions	Optional. Liste der zulässigen Berechtigungen. Geben Sie eine der folgenden Berechtigungen durch Leerzeichen getrennt ein: <ul style="list-style-type: none"> <li>- View. Benutzer können die Anwendung anzeigen.</li> <li>- Grant. Benutzer können Berechtigungen für die Anwendung gewähren und entziehen.</li> <li>- Execute. Benutzer können die Anwendung ausführen.</li> </ul>
-DeniedPermissions -dp	denied_permissions	Optional. Liste der Berechtigungen, die Benutzern verweigert werden sollen. Trennen Sie jeden Parameter durch ein Leerzeichen. Geben Sie eine der folgenden Berechtigungen durch Leerzeichen getrennt ein: <ul style="list-style-type: none"> <li>- View. Benutzer können die Anwendung anzeigen.</li> <li>- Grant. Benutzer können Berechtigungen für die Anwendung weder gewähren noch entziehen.</li> <li>- Execute. Benutzer können die Anwendung nicht ausführen.</li> </ul>

## setMappingExecutionEnvironment

Gibt die Mapping-Ausführungsumgebung für Mappings an, die im Datenintegrationsdienst bereitgestellt werden.

Verwenden Sie Filter, um eine Liste von Mappings, alle Mappings in einer Anwendung oder alle Anwendungen anzugeben, die für einen Datenintegrationsdienst bereitgestellt werden. Wenn Sie keine Filter einschließen, aktualisiert der Befehl alle Mappings, die im Datenintegrationsdienst bereitgestellt werden. Damit ein Mapping geändert werden kann, muss es allen festgelegten Filtern entsprechen.

Änderungen werden wirksam, nachdem Sie den Datenintegrationsdienst wiederverwendet haben.

Der Befehl `infacmd` `dis` `setMappingExecutionEnvironment` verwendet die folgende Syntax:

```
setMappingExecutionEnvironment
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-ProjectName|-pn> project_name]
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-MappingNamesFilter|-mnf> mapping_names]
<-ExecutionEnvironment|-ee> execution_environment_name
```

In der folgenden Tabelle werden die Optionen und Argumente von `setMappingExecutionEnvironment` beschrieben:

Option	Argument	Beschreibung
DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
Passwort -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-ProjectName -pn	project_name	Optional. Name des Projekts, das die Zuordnung enthält. Wenn Sie keinen Projektnamen angeben, aktualisiert der Befehl alle Projekte im Modellrepository.
MappingNamesFilter -mnf	mapping_names	Optional. Die Namen der Mappings, für die Sie die Ausführungsumgebung festlegen möchten. Trennen Sie die Namen der Mappings durch Kommas. Standardmäßig werden alle Mappings berücksichtigt, die für den Datenintegrationsdienst bereitgestellt werden.
ExecutionEnvironment -ee	execution_environment_name	Erforderlich. Identifiziert die festzulegende Ausführungsumgebung. Wählen Sie entweder „Nativ“, „Hadoop“ oder „Databricks“ aus.
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
NewConnectionName -nc	connection_name_of_new_connection	Erforderlich. Name der Hadoop- oder Databricks-Verbindung, die vom Datenintegrationsdienst verwendet werden muss, um eine Verbindung mit dem Computing-Cluster zur Ausführung von Zuordnungen in der nicht-nativen Umgebung herzustellen.

## SetSequenceState

Aktualisiert den aktuellen Wert des Sequenzdatenobjekts.

Der Befehl „infacmd dis SetSequenceState“ verwendet die folgende Syntax:

```
SetSequenceState
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
<-SequenceObjectPath|-sop> sequence_object_path
```

<-SequenceValue|-sv> sequence\_value

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis SetSequenceState“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Integrationsdiensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 230 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten: / * ? < > "
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-Application -a	application	Erforderlich. Name der Anwendung.

Option	Argument	Beschreibung
-SequenceObjectPath -sop	Sequenzobjekt-Pfad	<p>Erforderlich. Pfad zum Sequenzdatenobjekt. Der Pfad kann die folgenden Objekte in der angegebenen Reihenfolge (und wo zutreffend) enthalten:</p> <ul style="list-style-type: none"> <li>- Projekt</li> <li>- Ordner</li> <li>- SQL-Datendienst oder Webdienst</li> <li>- Mapping</li> <li>- Sequenzgeneratorumwandlung</li> <li>- Sequenzdatenobjekt</li> </ul> <p>Wenn Sie ein wiederverwendbares Sequenzdatenobjekt aktualisieren möchten, geben Sie den Pfad nur unter Verwendung des Projekts, der Ordner und des Sequenzdatenobjekts an.</p> <p>Wenn Sie ein nicht wiederverwendbares Sequenzdatenobjekt aktualisieren möchten, das sich in einem SQL-Datendienst oder einem Webdienst befindet, geben Sie vor dem SQL-Datendienst- oder Webdienstnamen ein Präfix an. Verwenden Sie die folgenden Präfixe mit Optionen im Befehl:</p> <ul style="list-style-type: none"> <li>- SQLEP:&lt;SQL-Datendienstname&gt;</li> <li>- WSEP:&lt;Webdienstname&gt;</li> </ul> <p>Trennen Sie die Optionen mit einem Schrägstrich (/).</p> <p><b>Beispiel:</b></p> <pre>&lt;Projektname&gt;/&lt;Ordnername&gt;/ WSEP:&lt;Webdienstname&gt;/&lt;Name der Operationszuordnung&gt;/&lt;Name der Sequenzgenerator-Transformation&gt;/&lt;Name des Sequenzdatenobjekts&gt;</pre>
-SequenceValue -sv	sequence_value	<p>Erforderlich. Der neue Wert für Sequenzdatenobjekt. Geben Sie einen Wert ein, der größer oder gleich dem Startwert des Sequenzdatenobjekts und kleiner oder gleich dem Endwert ist.</p>

## StartApplication

Startet eine bereitgestellte Anwendung. Sie müssen die Anwendung vor dem Starten aktivieren. Der Datenintegrationsdienst muss ausgeführt werden.

Der Befehl „infacmd dis StartApplication“ verwendet die folgende Syntax:

```
StartApplication
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
```



```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
<-Application|-a> application
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd startApplication“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	anwendung	Erforderlich. Name der zu startenden Anwendung.

## StopApplication

Hält eine Anwendung an. Sie können eine Anwendung anhalten, wenn sie gesichert werden muss oder wenn Benutzern der Zugriff auf die Anwendung verweigert werden soll.

Der Befehl „infacmd dis StopApplication“ verwendet die folgende Syntax:

```
StopApplication
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Application|-a> application
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis StopApplication“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-Application -a	anwendung	Erforderlich. Name der anzuhaltenden Anwendung.

## stopBlazeService

Stoppt die Komponenten der Blaze-Engine. Sie möchten die Ausführung der Blaze-Engine-Komponenten unter Umständen anhalten, wenn Sie den Hadoop-Cluster warten, wie z. B. beim Bereinigen von Ressourcen oder Anwenden von Software-Patches.

Der `infacmd` `dis stopBlazeService`-Befehl verwendet die folgende Syntax:

```
stopBlazeService
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-HadoopConnection|-hc> Hadoop_Cluster_Connection_Name
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd` `dis stopBlazeService`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option <code>-dn</code> oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option <code>-dn</code> Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-HadoopConnection -hc	Hadoop_Cluster_Connection_Name	Erforderlich. Name der Hadoop-Verbindung, die der Datenintegrationsdienst zum Ausführen der Zuordnung auf der Blaze-Engine verwendet.

**Hinweis:** Beim Ausführen des Befehls „stopBlazeService“ werden bestimmte Komponentenprotokolle unter Umständen nicht in aggregierte Protokolldateien auf HDFS geschrieben. Sie können die Protokolle in dem für die Blaze-Engine-Protokolle konfigurierten Verzeichnis anzeigen, das auf der folgenden erweiterten Blaze-Eigenschaft in der Hadoop-Verbindung basiert: `infagrid.node.local.root.log.dir`.

## Tag

Weist Tags Entwurfszeitobjekten zu.

Tags sind Metadaten, die ein Objekt im Modellrepository-Dienst definieren. Fragen Sie die Objekte ab und geben Sie die Tags zur Gruppierung der Objekte entsprechend ihrer geschäftlichen Nutzung an. Wenn Sie einem Objekt ein Tag neu zuweisen, überschreibt der Befehl das vorhandene Tag.

Der Befehl „infacmd dis tag“ verwendet die folgende Syntax:

```
tag
<-DomainName|-dn> domain_name

<-ServiceName|-sn> DIS_service_name

<-UserName|-un> DIS_user_name

<-Password|-pd> DIS_password

[<-SecurityDomain|-sdn> DIS_security_domain]

<-RepositoryService|-rs> MRS_service_name

<-RepositoryUserName|-rsun> MRS_user_name

<-RepositoryPassword|-rspd> MRS_password

[<-RepositorySecurityDomain|-rssdn> MRS_security_domain]
```

```

<-Query|-q> Query

<-TagName|-tn> tag_name

[<-TagDescription|-td> tag_description]

[<-TimeZone|-tz> time_zone]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis tag“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	DIS-Dienstname	Erforderlich. Name des Datenintegrationsdiensts.
-UserName -un	DIS-Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	DIS-Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	DIS-Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.
RepositoryService -rs	MRS-Dienstname	Erforderlich. Name des Modellrepository-Diensts.



Option	Argument	Beschreibung
-RepositoryUserName -rsun	MRS-Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -rsun oder der Umgebungsvariablen INFA_REPOSITORY_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -rsun Vorrang.
-RepositoryPassword -rspd	MRS-Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -rspd oder der Umgebungsvariablen INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-rspd“ festgelegte Passwort Vorrang.
RepositorySecurityDomain -rssdn	MRS-Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -rssdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -rssdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.
-Query -q	Abfrage	Erforderlich. Eine Zeichenfolge, die das Repository nach einem Tag-Namen abfragt. Weitere Informationen hierzu finden Sie unter <a href="#">"Abfragen" auf Seite 290</a> .
-TagName -tn	Tag-Name	Erforderlich. Name des Tags, das Sie dem abgefragten Objekt zuweisen möchten. Der Name darf maximal 128 Zeichen umfassen und muss mit einer Zahl beginnen. Der Name muss aus alphanumerischen Zeichen bestehen. Sie können auch Sonderzeichen wie @ # _ verwenden.

Option	Argument	Beschreibung
-TagDescription -td	Tag-Beschreibung	Optional. Die Beschreibung des Tags.
-TimeZone -tz	Zeitzone	Optional. Standardmäßig verwendet der Befehl die Zeitzone auf dem Computer, auf dem der Datenintegrationsdienstprozess ausgeführt wird. Eine Liste der gültigen Zeitzonen finden Sie in der Klasse „java.time.ZoneID“.

## untag

Entfernt Tags von Entwurfszeitobjekten.

Wenn sich die geschäftliche Nutzung geändert hat, entfernen Sie die Tags, um die Gruppierung von Objekten aufzuheben. Fragen Sie die Objekte ab und geben Sie die zu entfernenden Tags an.

Der Befehl „infacmd dis untag“ verwendet die folgende Syntax:

```

untag
<-DomainName|-dn> domain_name

<-ServiceName|-sn> DIS_service_name

<-UserName|-un> DIS_user_name

<-Password|-pd> DIS_password

[<-SecurityDomain|-sdn> DIS_security_domain]

<-RepositoryService|-rs> MRS_service_name

<-RepositoryUserName|-rsun> MRS_user_name

<-RepositoryPassword|-rspd> MRS_password

[<-RepositorySecurityDomain|-rssdn> MRS_security_domain]

<-Query|-q> Query

<-TagName|-tn> tag_name

[<-TimeZone|-tz> time_zone]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis untag“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	DIS-Dienstname	Erforderlich. Name des Datenintegrationsdiensts.

Option	Argument	Beschreibung
-UserName -un	DIS-Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	DIS-Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	DIS-Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.
-RepositoryService -rs	MRS-Dienstname	Erforderlich. Name des Modellrepository-Diensts.
-RepositoryUserName -rsun	MRS-Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -rsun oder der Umgebungsvariablen INFA_REPOSITORY_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -rsun Vorrang.

Option	Argument	Beschreibung
-RepositoryPassword -rspd	MRS-Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -rspd oder der Umgebungsvariablen INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-rspd“ festgelegte Passwort Vorrang.
-RepositorySecurityDomain -rssdn	MRS-Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -rssdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -rssdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.
-Query -q	Abfrage	Erforderlich. Eine Zeichenfolge, die das Repository nach einem Tag-Namen abfragt. Weitere Informationen hierzu finden Sie unter <a href="#">„Abfragen“ auf Seite 290</a> .
-TagName -tn	Tag-Name	Erforderlich. Name des Tags, das Sie aus dem abgefragten Objekt entfernen möchten.
-TimeZone -tz	Zeitzone	Optional. Standardmäßig verwendet der Befehl die Zeitzone auf dem Computer, auf dem der Datenintegrationsdienstprozess ausgeführt wird. Eine Liste der gültigen Zeitzonen finden Sie in der Klasse „java.time.ZoneID“.

## replaceAllTag

Ersetzt alle Tags, die Entwurfszeitobjekten zugewiesen sind.

Fragt die Objekte ab und ersetzt die zugewiesenen Tags. Wenn sich die geschäftliche Nutzung geändert hat, können Sie den Befehl zum Aufheben der Gruppierung von Objekten verwenden und neue Tags zum Umgruppieren von Objekten zuweisen. Alle zugewiesenen Tags werden gelöscht und durch das angegebene Tag ersetzt.

Der Befehl „infacmd dis replaceAllTag“ verwendet die folgende Syntax:

```
replaceAllTag
<-DomainName|-dn> domain_name

<-ServiceName|-sn> DIS_service_name

<-UserName|-un> DIS_user_name

<-Password|-pd> DIS_password

[<-SecurityDomain|-sdn> DIS_security_domain]

<-RepositoryService|-rs> MRS_service_name

<-RepositoryUserName|-rsun> MRS_user_name

<-RepositoryPassword|-rspd> MRS_password

[<-RepositorySecurityDomain|-rssdn> MRS_security_domain]

<-Query|-q> Query

<-TagName|-tn> tag_name

[<-TagDescription|-td> tag_description]

[<-TimeZone|-tz> time_zone]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis replaceAllTag“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	DIS-Dienstname	Erforderlich. Name des Datenintegrationsdiensts.
-UserName -un	DIS-Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	DIS-Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/ Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	DIS-Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.
-RepositoryService -rs	MRS-Dienstname	Erforderlich. Name des Modellrepository-Diensts.
-RepositoryUserName -rsun	MRS-Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -rsun oder der Umgebungsvariablen INFA_REPOSITORY_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -rsun Vorrang.
-RepositoryPassword -rspd	MRS-Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -rspd oder der Umgebungsvariablen INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-rspd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-RepositorySecurityDomain -rssdn	MRS-Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -rssdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -rssdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.
-Query -q	query	Erforderlich. Eine Zeichenfolge, die das Repository nach einem Tag-Namen abfragt. Weitere Informationen hierzu finden Sie unter <a href="#">"Abfragen" auf Seite 290</a> .
-TagName -tn	Tag-Name	Erforderlich. Der Name des Ersetzungs-Tags, das Sie den abgefragten Objekten zuweisen möchten. Der Name darf maximal 128 Zeichen umfassen und muss mit einer Zahl beginnen. Der Name muss aus alphanumerischen Zeichen bestehen. Sie können auch Sonderzeichen wie @ # _ verwenden.
-TagDescription -td	Tag-Beschreibung	Optional. Die Beschreibung des Tags.
-TimeZone -tz	Zeitzone	Optional. Standardmäßig verwendet der Befehl die Zeitzone auf dem Computer, auf dem der Datenintegrationsdienstprozess ausgeführt wird. Eine Liste der gültigen Zeitzonen finden Sie in der Klasse „java.time.ZoneID“.

## UndeployApplication

Entfernt eine Anwendung aus einem Datenintegrationsdienst.

Der Befehl „infacmd dis UndeployApplication“ verwendet die folgende Syntax:

```
UndeployApplication
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
```

```

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-Application|-a> application

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis UndeployApplication“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.



Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, aus dem die Anwendung entfernt wird.
-Application -a	anwendung	Erforderlich. Name der Anwendung, die aus dem Datenintegrationsdienst entfernt wird.

## UpdateApplication

Aktualisiert eine Anwendung über eine Anwendungsdatei und verwaltet die Konfiguration. Die Anwendung muss in einem Datenintegrationsdienst bereitgestellt werden. Endanwender können auf die neueste Version der Anwendung zugreifen.

Der Befehl „infacmd dis UpdateApplication“ verwendet die folgende Syntax:

```
UpdateApplication
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-FileName|-f> file_name
[<-Application|-a> application]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis UpdateApplication“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	Passwort	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-FileName -f	file_name	<p>Erforderlich. Name und Pfad der Anwendungsdatei, mit der die bereitgestellte Anwendung aktualisiert wird.</p>
-Application -a	anwendung	<p>Optional. Name der bereitgestellten Anwendung.</p>

# UpdateApplicationOptions

Aktualisiert die Anwendungseigenschaften.

Trennen Sie die einzelnen Optionen und Werte mit einem Leerzeichen. Führen Sie zum Anzeigen der aktuellen Eigenschaften `infacmd` das `ListApplicationOptions` aus.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Der Befehl „`infacmd` das `UpdateApplicationOptions`“ verwendet die folgende Syntax:

```
UpdateApplicationOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd` das `UpdateApplicationOptions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	anwendung	Erforderlich. Name der zu aktualisierenden Anwendung.
-Options -o	optionen	Erforderlich. Geben Sie alle zu aktualisierenden Optionen und Werte ein. Trennen Sie jede Option mit einem Leerzeichen. Führen Sie zum Anzeigen der Anwendungsoptionen den infacmd dis ListApplicationOptions-Befehl aus.

## UpdateComputeOptions

Aktualisiert Datenintegrationsdienst-Eigenschaften für einen Knoten mit der Berechnungsrolle. Verwenden Sie den Befehl, um Datenintegrationsdienst-Eigenschaften für einen bestimmten Berechnungsknoten zu überschreiben.

Geben Sie die Optionen in folgendem Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Der `infacmd` des `UpdateComputeOptions`-Befehls verwendet die folgende Syntax:

```
UpdateComputeOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd` des `UpdateComputeOptions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domännennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domännennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
NodeName -nn	node_name	Erforderlich. Knoten mit der Berechnungsrolle, die dem Datenintegrationsdienst oder dem Datenintegrationsdienstgitter zugewiesen ist.
-Options -o	options	<p>Erforderlich. Geben Sie jede Option durch ein Leerzeichen getrennt ein. Führen Sie zum Anzeigen der Optionen den infacmd dis ListComputeOptions-Befehl aus.</p> <p>Sie können die folgenden Optionen des Datenintegrationsdiensts aktualisieren:</p> <ul style="list-style-type: none"> <li>- ExecutionOptions.TemporaryDirectories</li> <li>- ExecutionOptions.DISHomeDirectory</li> <li>- ExecutionOptions.CacheDirectory</li> <li>- ExecutionOptions.SourceDirectory</li> <li>- ExecutionOptions.TargetDirectory</li> <li>- ExecutionOptions.RejectFilesDirectory</li> </ul>

## UpdateDataObjectOptions

Aktualisiert Datenobjekteigenschaften. Führen Sie den infacmd dis ListDataObjectOptions-Befehl aus, um die aktuellen Optionen anzuzeigen.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Der Befehl „`infacmd dis UpdateDataObjectOptions`“ verwendet die folgende Syntax:

```
UpdateDataObjectOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
<-Folder|-f> folder
<-DataObject|-do> data_model.data_object
<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd dis UpdateDataObjectOptions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	anwendung	Erforderlich. Anwendung, in der das Datenobjekt enthalten ist.
-Folder -f	Folder	Erforderlich. Name des Ordners, der das Datenobjektmodell enthält.
-DataObject -do	data_model.data_object	Erforderlich. Name des Datenobjekts, das Sie aktualisieren möchten.
-Options -o	optionen	Erforderlich. Geben Sie Optionen und Werte durch Leerzeichen getrennt ein. Führen Sie den infacmd dis ListDataObjectOptions-Befehl aus, um die aktuellen Optionen anzuzeigen.

## Datenobjektoptionen

Verwenden Sie die Datenobjektoptionen, um das Zwischenspeichern für ein logisches Datenobjekt zu konfigurieren. Verwenden Sie die Datenobjektoptionen mit dem infacmd dis UpdateDataObjectOptions-Befehl.

Geben Sie Datenobjektoptionen im folgenden Format ein:

```
... -o option_type.option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.



Die folgende Tabelle beschreibt die Datenobjektoptionen:

Option	Beschreibung
DataObjectOptions.CachingEnabled	Zwischenspeichern des logischen Datenobjekts in der Cache-Datenbank des Datenobjekts. „True“ oder „False“. Standardwert ist „True“.
DataObjectOptions.CacheRefreshPeriod	Anzahl der Minuten zwischen den Cache-Aktualisierungen. Standardwert ist Null.
DataObjectOptions.CacheTableName	<p>Der Name der benutzerverwalteten Tabelle, aus der der Datenintegrationsdienst auf den Cache des logischen Datenobjekts zugreift. Eine benutzerverwaltete Cache-Tabelle ist eine Tabelle in der Cache-Datenbank des Datenobjekts, die Sie bei Bedarf erstellen, füllen und manuell aktualisieren können.</p> <p>Wenn Sie einen Cache-Tabellennamen angeben, verwaltet der Datenobjekt-Cache-Manager den Cache für das Objekt nicht und ignoriert den Cache-Aktualisierungszeitraum. Wenn Sie keinen Cache-Tabellennamen angeben, verwaltet der Datenobjekt-Cache-Manager den Cache für das Objekt.</p>

## UpdateParameterSetEntries

Aktualisiert Einträge aus einem Parametersatz. Führen Sie diesen Befehl aus, um die Werte in Parametersatzeinträgen für eine Zuordnung oder einen Arbeitsablauf in einer Anwendung zu aktualisieren.

Der infacmd-Befehl `dis UpdateParameterSetEntries` verwendet die folgende Syntax:

```
UpdateParameterSetEntries
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
<-parameterSetName|-ps> parameter set name
<-projectScope|-prs> path to the mapping or workflow that contains the parameters. For a
mapping, M1, in project P1 and folder F1, the path is P1/F1/mapping/M1.
<-paramNames|-pnv> parameter name-value pairs, separated by double quotes
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis UpdateParameterSetEntries“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application	Erforderlich. Name der Anwendung, die den Parametersatz enthält.
parametersetname -ps	parameterset name	Erforderlich. Name des Parametersatzes.
-projectScope -prs	project scope	Erforderlich. Pfad der Zuordnung oder des Arbeitsablaufs, der die Parameter enthält. Für die Zuordnung M1 in Projekt P1 und Ordner F1 lautet der Pfad: P1/F1/Zuordnung/M1.
-paramNames -pnv	parameter names	Erforderlich. Namen-Wert-Paare des Parameters getrennt durch Leerzeichen. Setzen Sie Namen-Wert-Paare in doppelte Anführungszeichen. Versehen Sie jeden Wert mit einfachen Anführungszeichen. Verwenden Sie folgende Syntax: "parm1='valueA'" "parm2='valueB'" "parm3='valueC'" . Sie können Leerzeichen in einem Parameterwert verwenden. Sie können ein Apostroph (') oder einen Doppelpunkt (:) im Wert verwenden, wenn Sie für diese Zeichen einen umgekehrten Schrägstrich (\) als Escape-Zeichen verwenden. 'C:\Verzeichnis'

## UpdateServiceOptions

Aktualisiert Datenintegrationsdienst-Eigenschaften. Führen Sie zum Anzeigen der aktuellen Eigenschaften den infacmd `listServiceOptions`-Befehl aus.

Sie können Diensteseigenschaften und den Dienst zur Ausführung auf einem Einzelknoten oder Raster ändern. Änderungen werden nach dem Wiederherstellen des Diensts wirksam. Sie können die Option `-rm` (`RecycleMode`) zum Recyceln des Diensts verwenden.

```
UpdateServiceOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-Options|-o> options]
```

```
[<-nodeName|-nn> node_name | <-GridName|-gn> grid_name]
```

```
[<-RecycleMode|-rm> recycle_mode]
```

```
[<-BackupNodes|-bn> node_name1,node_name2,...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis UpdateServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Options -o	options	Optional. Geben Sie jede Option durch ein Leerzeichen getrennt ein. Führen Sie zum Anzeigen der Optionen den Befehl „infacmd dis ListServiceOptions“ aus.
-NodeName -nn	node_name	Wenn Sie den Datenintegrationsdienst aus einem Raster entfernen und auf einem Einzelknoten ausführen möchten, geben Sie den Knotennamen ein. Sie können entweder den Knoten- oder den Rasternamen eingeben.
-GridName -gn	grid_name	Wenn Sie den Datenintegrationsdienst von einem Einzelknoten in ein Raster verschieben möchten, geben Sie den Namen des Rasters ein. Sie können entweder den Knoten- oder den Rasternamen eingeben.
-RecycleMode -rm	recycle_mode	Optional. Der Wiederherstellungsmodus startet den Dienst neu und wendet den aktuellen Dienst und die aktuellen Dienstvorgangseigenschaften an. Wählen Sie „Abbrechen“ oder „Abschließen“ aus. <ul style="list-style-type: none"> <li>- Abschließen. Stoppt alle Anwendungen und bricht alle Jobs in sämtlichen Anwendungen ab. Wartet vor der Deaktivierung des Diensts, bis alle Jobs abgebrochen wurden.</li> <li>- Abbrechen. Stoppt alle Anwendungen und versucht, alle Jobs vor deren Abbruch und Deaktivieren des Diensts anzuhalten.</li> </ul> Standardwert ist „Abschließen“.
-BackupNodes -bn	node_name1,node_name2,.. ..	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Backup-Knoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.

## Optionen des Datenintegrationsdiensts

Verwenden Sie die Optionen des Datenintegrationsdiensts mit dem infacmd dis-Befehl UpdateServiceOptions.

Geben Sie die Optionen des Datenintegrationsdiensts in folgendem Format ein:

```
... -o option_type.option_name=value
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Optionen des Datenintegrationsdiensts beschrieben:

Option	Beschreibung
AdvancedProfilingServiceOptions.ColumnsPerMapping	Begrenzt die Anzahl der Spalten, für die in einer einzelnen Zuordnung ein Profil erstellt werden kann, um Arbeits- und Festplattenspeicher einzusparen. Standardwert ist 5. Wenn Sie ein Profil für eine Quelle mit über 100 Millionen Zeilen erstellen, verringern Sie den Wert auf 1.
AdvancedProfilingServiceOptions.ExecutionPoolSize	Maximale Anzahl an Threads zum Ausführen von Zuordnungen.
AdvancedProfilingServiceOptions.MaxMemPerRequest	Die maximale Speichermenge in Byte, die der Datenintegrationsdienst für jede Mapping-Ausführung für eine einzelne Profilanfrage zuordnen kann. Standardwert ist 536.870.912.
AdvancedProfilingServiceOptions.MaxNumericPrecision	Maximale Anzahl an Ziffern für einen numerischen Wert.
AdvancedProfilingServiceOptions.MaxParallelColumnBatches	Anzahl der Threads, die gleichzeitig Zuordnungen ausführen können. Standardwert ist 1.
AdvancedProfilingServiceOptions.MaxStringLength	Maximale Länge einer Zeichenfolge, die vom Profilerstellungsdienst verarbeitet werden kann.
AdvancedProfilingServiceOptions.MaxValueFrequencyPairs	Maximale Anzahl an im Profiling Warehouse zu speichernden Wert-/Frequenzpaaren. Standardwert ist 16.000.
AdvancedProfilingServiceOptions.MinPatternFrequency	Mindestanzahl an Mustern, die für ein Profil angezeigt werden sollen.
AdvancedProfilingServiceOptions.ReservedThreads	Anzahl der Threads der maximalen Ausführungspoolgröße für Prioritätsanfragen. Standardwert ist 1.
AdvancedProfilingServiceOptions.ValueFrequencyMemSize	Zulässige Speichermenge für Wert-/Frequenzpaare. Standardwert ist 64 Megabyte.
DataObjectCacheOptions.CacheConnection	Der Datenbankverbindungsname für die Datenbank, in der der Datenobjekt-Cache gespeichert wird. Geben Sie einen gültigen Namen für das Verbindungsobjekt ein.
DataObjectCacheOptions.CacheRemovalTime	Die Anzahl von Millisekunden, die der Datenintegrationsdienst wartet, ehe er den Cache-Speicher nach einer Aktualisierung bereinigt. Standardwert ist 3.600.000.
DeploymentOptions.DefaultDeploymentMode	Gibt an, ob eine Anwendung aktiviert und gestartet werden soll, nachdem sie einem Datenintegrationsdienst bereitgestellt wurde. Geben Sie eine der folgenden Optionen ein: <ul style="list-style-type: none"> <li>- EnableandStart. Aktivieren und starten Sie die Anwendung.</li> <li>- EnableOnly. Aktivieren Sie die Anwendung, ohne sie zu starten.</li> <li>- Disable. Aktivieren Sie die Anwendung nicht.</li> </ul>

Option	Beschreibung
DataObjectCacheOptions.EnableNestedLDOCache	<p>Gibt an, dass der Datenintegrationsdienst Cache-Daten für ein logisches Datenobjekt verwenden kann, das während einer Cache-Aktualisierung in einem anderen logischen Datenobjekt als Quelle oder als Lookup verwendet wird. Bei false greift der Datenintegrationsdienst auf die Quellressourcen zu, auch wenn das Caching für das als Quelle oder Lookup verwendete logische Datenobjekt aktiviert wurde.</p> <p>Beispiel: Das logische Datenobjekt LDO3 vereint Daten aus den logischen Datenobjekten LDO1 und LDO2. Ein Entwickler erstellt ein Mapping, das LDO3 als Eingabe verwendet, und bezieht das Mapping in einer Anwendung mit ein. Sie aktivieren das Caching für LDO1, LDO2, LDO3. Wenn Sie das Caching für verschachtelte logische Datenobjekte aktivieren, verwendet der Datenintegrationsdienst bei der Aktualisierung der Cache-Tabelle für LDO3 auch Cache-Daten für LDO1 und LDO2. Wenn Sie das Caching für verschachtelte logische Datenobjekte nicht aktivieren, greift der Datenintegrationsdienst bei der Aktualisierung der Cache-Tabelle für LDO3 auf die Quellressourcen für LDO1 und LDO2 zu.</p> <p>Standardwert ist „false“.</p>
DataObjectCacheOptions.MaxConcurrentRefreshRequests	Maximale Anzahl an Cache-Aktualisierungen, die gleichzeitig stattfinden können.
ExecutionContextOptions.Spark.MSPEnableUnassignedData	<p>Wenn dieser Wert auf „True“ festgelegt ist, wird die Funktion „Midstream-Parsing“ aktiviert, die nicht geparte Daten in der Quellzeichenfolge erfasst und in einem Array vom Typ <code>UnassignedData</code> als <code>unidentifiedDataItem</code> speichert.</p> <p>Wenn der Parser auf ein Datenfeld trifft, das nicht gepart werden kann, werden die Daten in der Regel ignoriert. Das komplexe Datenschema der Quellzeichenfolge kann sich jedoch ändern. Mit einem Software-Update auf dem Server kann beispielsweise die JSON- oder XML-Datei geändert werden. Mit dieser Option können Sie Daten zu Analyse Zwecken erfassen.</p> <p>Der Standardwert ist „false“.</p>
ExecutionOptions.BigDataJobRecovery	<p>Wenn dieser Wert auf „True“ festgelegt ist, werden Data-Engineering-Jobwiederherstellung und verteiltes Queueing für bereitgestellte Jobs aktiviert, die zur Ausführung auf der Spark-Engine konfiguriert sind.</p> <p>Standardwert ist „False“.</p>
ExecutionOptions.CacheDirectory	<p>Verzeichnis für Index- und Daten-Cache-Dateien für Umwandlungen. Standardwert ist <code>&lt;Basisverzeichnis&gt;/cache</code>.</p> <p>Geben Sie eine Liste mit durch Semikola getrennten Verzeichnissen ein, um die Leistung während der Cache-Partitionierung für Aggregator-, Joiner- und Rangumwandlungen zu optimieren.</p> <p>Die folgenden Zeichen dürfen nicht im Verzeichnispfad verwendet werden:</p> <p>* ? &lt; &gt; "   ,</p>
ExecutionOptions.DisHadoopKeytab	Der Dateipfad der Kerberos-Keytab-Datei auf dem Computer, auf dem der Datenintegrationsdienst ausgeführt wird.

Option	Beschreibung
ExecutionOptions.DisHadoopPrincipal	Dienstprinzipalname (SPN) des Datenintegrationsdiensts zum Herstellen einer Verbindung zu einem Hadoop-Cluster, der Kerberos-Authentifizierung verwendet.
ExecutionOptions.DISHomeDirectory	<p>Root-Verzeichnis, auf das vom Knoten aus zugegriffen werden kann. Dies ist das Root-Verzeichnis für andere Dienstverzeichnisse. Standardwert ist &lt;Informatica-Installationsverzeichnis&gt;/tomcat/bin. Wenn Sie den Standardwert ändern, stellen Sie sicher, dass das Verzeichnis vorhanden ist.</p> <p>Die folgenden Zeichen dürfen nicht im Verzeichnispfad verwendet werden:</p> <p>* ? &lt; &gt; "   ,</p>
ExecutionOptions.EnableOSProfile	Gibt an, dass der Datenintegrationsdienst Betriebssystemprofile für die Ausführung von Zuordnungen verwenden kann. Sie können Betriebssystemprofile aktivieren, wenn der Datenintegrationsdienst unter UNIX oder Linux ausgeführt wird. Standardwert ist FALSE.
ExecutionOptions.HadoopDistributionDir	<p>Das Verzeichnis enthält eine Sammlung von Hadoop-JARS im Cluster aus den RPM-Installationsspeicherorten. Das Verzeichnis enthält den minimalen Satz an JARs, die für die Verarbeitung von Informatica-Mappings in einer Hadoop-Umgebung erforderlich sind. Geben Sie /</p> <p>&lt;PowerCenterBigDataEditionInstallationDirectory&gt;/Informatica/services/shared/hadoop/[Hadoop_distribution_name] ein.</p>
ExecutionOptions.HadoopInfaHomeDir	<p>Das PowerCenter Big Data Edition-Basisverzeichnis auf jedem von der Hadoop RPM-Installation erstellten Datenknoten. Geben Sie /</p> <p>&lt;PowerCenterBigDataEditionInstallationDirectory&gt;/Informatica ein.</p>
ExecutionOptions.MaxHadoopBatchExecutionPool Size	Maximale Anzahl an bereitgestellten Jobs, die gleichzeitig in der Hadoop-Umgebung ausgeführt werden können. Der Datenintegrationsdienst verschiebt Hadoop-Jobs aus der Warteschlange in den Hadoop-Job-Pool, wenn genügend Ressourcen verfügbar sind. Standardwert ist 100.



Option	Beschreibung
ExecutionOptions.MaxMappingParallelism	<p>Maximale Anzahl paralleler Threads, die eine einzelne Zuordnungs-Pipeline-Stage verarbeiten.</p> <p>Wenn Sie den Wert auf größer als eins festlegen, aktiviert der Datenintegrationsdienst Partitionierung für Zuordnungen sowie für aus Profilen umgewandelte Zuordnungen. Der Dienst führt eine dynamische Skalierung der Anzahl an Partitionen für eine Zuordnungs-Pipeline zur Laufzeit durch. Erhöhen Sie den Wert basierend auf der Anzahl der CPUs, die auf den Knoten verfügbar sind, auf denen Zuordnungen ausgeführt werden.</p> <p>Im Developer Tool können Entwickler den Wert für den maximalen Parallelismus je Zuordnung festlegen. Wenn maximaler Parallelismus sowohl für den Datenintegrationsdienstprozess als auch für die Zuordnung eingerichtet wurde, verwendet der Datenintegrationsdienst den Minimalwert beim Ausführen der Zuordnung.</p> <p>Standardwert ist 1. Maximalwert ist 64.</p>
ExecutionOptions.MaxMemorySize	<p>Die maximale Speichermenge in Byte, die der Datenintegrationsdienst für die gleichzeitige Ausführung aller Anfragen zuordnen kann, wenn der Dienst Jobs in dem Prozess des Datenintegrationsdiensts ausführt. Wenn der Datenintegrationsdienst Jobs in separaten lokalen Prozessen oder Remoteprozessen ausführt, ignoriert der Dienst diesen Wert. Wenn Sie die Speichergröße, die der Datenintegrationsdienst zuordnen kann, nicht einschränken möchten, legen Sie diese Eigenschaft auf 0 fest.</p> <p>Wenn der Wert größer als 0 ist, verwendet der Datenintegrationsdienst die Eigenschaft zur Berechnung des maximalen Gesamtspeicherplatzes, der für die gleichzeitige Ausführung aller Anfragen zulässig ist. Der Datenintegrationsdienst berechnet den maximalen Gesamtspeicherplatz folgendermaßen:</p> <p>Maximale Speichergröße + maximale Heap-Größe + zum Laden von Programmkomponenten erforderlicher Speicherplatz</p> <p>Standardwert ist 0.</p> <p><b>Hinweis:</b> Wenn Sie Profile oder Datenqualitäts-Mappings ausführen, müssen Sie diese Eigenschaft auf 0 festlegen.</p>
ExecutionOptions.MaxNativeBatchExecutionPoolSize	<p>Maximale Anzahl an bereitgestellten Jobs, die gleichzeitig in der nativen Umgebung ausgeführt werden können. Der Datenintegrationsdienst verschiebt native Zuordnungsjobs aus der Warteschlange in den nativen Job-Pool, wenn genügend Ressourcen verfügbar sind. Standardwert ist 10.</p>
ExecutionOptions.MaxOnDemandExecutionPoolSize	<p>Maximale Anzahl an auf Abruf verfügbaren Jobs, die gleichzeitig ausgeführt werden können. Zu den Jobs gehören Datenvorschauen, Profilerstellungsjobs, REST- und SQL-Abfragen, Webdienstanfragen und Zuordnungen, die vom Developer Tool ausgeführt werden. Alle Jobs, die der Datenintegrationsdienst empfängt, tragen zur Größe des bedarfsabhängigen Pools bei. Der Datenintegrationsdienst führt auf Abruf verfügbare Jobs sofort aus, wenn genügend Ressourcen vorhanden sind. Andernfalls lehnt der Datenintegrationsdienst den Job ab. Standardwert ist 10.</p>

Option	Beschreibung
ExecutionOptions.OutOfProcessExecution	<p>Führt Jobs im Datenintegrationsdienstprozess, in separaten DTM-Prozessen auf dem lokalen Knoten oder in separaten DTM-Prozessen auf Remoteknoten aus. Konfigurieren Sie die Eigenschaft basierend auf den vom Datenintegrationsdienst ausgeführten Jobtypen sowie basierend darauf, ob der Datenintegrationsdienst auf einem Einzelknoten oder Gitter ausgeführt wird.</p> <p>Geben Sie eine der folgenden Optionen ein:</p> <ul style="list-style-type: none"> <li>- IN_PROCESS. Führt Jobs im Datenintegrationsdienstprozess aus. Konfigurieren Sie diese Option, wenn Sie Jobs des SQL-Datendienstes und des Webdiensts auf einem Einzelknoten oder Gitter ausführen, in dem jeder Knoten sowohl über die Dienst- als auch über die Berechnungsrolle verfügt.</li> <li>- OUT_OF_PROCESS. Führt Jobs in separaten DTM-Prozessen auf dem lokalen Knoten aus. Konfigurieren Sie diese Option, wenn Sie Zuordnungs-, Profil- und Arbeitsablaufjobs auf einem Einzelknoten oder Gitter ausführen, in dem jeder Knoten sowohl über die Dienst- als auch über die Berechnungsrolle verfügt.</li> <li>- OUT_OF_PROCESS_REMOTE. Führt Jobs in separaten DTM-Prozessen auf Remoteknoten aus. Konfigurieren Sie diese Option, wenn Sie Zuordnungs-, Profil- und Arbeitsablaufjobs auf einem Gitter ausführen, in dem Knoten eine andere Kombination der Rollen aufweisen können. Wenn Sie diese Option konfigurieren und der Datenintegrationsdienst auf einem Einzelknoten ausgeführt wird, führt der Dienst Jobs in separaten lokalen Prozessen aus.</li> </ul> <p>Standardwert ist OUT_OF_PROCESS.</p>
ExecutionOptions.RejectFilesDirectory	<p>Verzeichnis für Ablehnungsdateien. Ablehnungsdateien enthalten Zeilen, die beim Ausführen eines Mappings zurückgewiesen wurden. Standardwert ist &lt;Basisverzeichnis&gt;/reject.</p> <p>Die folgenden Zeichen dürfen nicht im Verzeichnispfad verwendet werden:</p> <p>* ? &lt; &gt; "   ,</p>
ExecutionOptions.SourceDirectory	<p>Verzeichnis für Einfachdateien der Quelle, die in einem Mapping verwendet werden. Standardwert ist &lt;Basisverzeichnis&gt;/source.</p> <p>Wenn der Datenintegrationsdienst auf einem Gitter ausgeführt wird, können Sie ein freigegebenes Verzeichnis zum Erstellen eines Verzeichnisses für Quelldateien verwenden. Wenn Sie für jeden Knoten mit der Berechnungsrolle ein anderes Verzeichnis konfigurieren, stellen Sie sicher, dass die Quelldateien in allen Quellverzeichnissen konsistent sind.</p> <p>Die folgenden Zeichen dürfen nicht im Verzeichnispfad verwendet werden:</p> <p>* ? &lt; &gt; "   ,</p>

Option	Beschreibung
ExecutionOptions.TargetDirectory	<p>Standardverzeichnis für Zieleinfachdateien, die in einem Mapping verwendet werden. Standardwert ist &lt;Basisverzeichnis&gt;/target.</p> <p>Geben Sie eine Liste mit durch Semikola getrennten Verzeichnissen ein, um die Leistung zu steigern, wenn mehrere Partitionen in das Einfachdateiziel schreiben.</p> <p>Wenn der Datenintegrationsdienst auf einem Gitter ausgeführt wird, verwenden Sie zum Erstellen eines Verzeichnisses für Zieldateien ein freigegebenes Verzeichnis. Wenn Sie für jeden Knoten mit der Berechnungsrolle ein anderes Verzeichnis konfigurieren, stellen Sie sicher, dass die Zieldateien in allen Zielverzeichnissen konsistent sind.</p> <p>Die folgenden Zeichen dürfen nicht im Verzeichnispfad verwendet werden:</p> <p>* ? &lt; &gt; "   ,</p>
ExecutionOptions.TemporaryDirectories	<p>Verzeichnis für temporäre Dateien, die während der Ausführung von Jobs erstellt werden. Standardwert ist &lt;Basisverzeichnis&gt;/disTemp.</p> <p>Geben Sie eine Liste mit durch Semikola getrennten Verzeichnissen ein, um die Leistung während Profilvorgängen und während der Cache-Partitionierung für Sortierumwandlungen zu optimieren.</p> <p>Die folgenden Zeichen dürfen nicht im Verzeichnispfad verwendet werden:</p> <p>* ? &lt; &gt; "   , [ ]</p>
HttpConfigurationOptions.AllowedHostNames	<p>Liste der Konstanten oder regulären Java-Expressionsmuster im Vergleich zu den Hostnamen des anfragenden Computers. Die Hostnamen unterliegen der Groß-/Kleinschreibung. Trennen Sie mehrere Konstanten oder Expressionen durch ein Leerzeichen.</p> <p>Wenn Sie diese Eigenschaft konfigurieren, nimmt der Datenintegrationsdienst Anfragen von Hosts an, deren Namen mit dem Muster der zulässigen Hostnamen übereinstimmen.</p> <p>Wenn Sie diese Eigenschaft nicht konfigurieren, verwendet der Datenintegrationsdienst die Eigenschaft „Abgelehnte Hostnamen“ zum Bestimmen der Clients, die Anfragen senden können.</p>
HttpConfigurationOptions.AllowedIPAddresses	<p>Liste der Konstanten oder regulären Java-Expressionsmuster im Vergleich zur IP-Adresse des anfragenden Computers. Trennen Sie mehrere Konstanten oder Expressionen durch ein Leerzeichen.</p> <p>Wenn Sie diese Eigenschaft konfigurieren, nimmt der Datenintegrationsdienst Anfragen von IP-Adressen an, die mit dem zulässigen Adressmuster übereinstimmen. Wenn Sie diese Eigenschaft nicht konfigurieren, verwendet der Datenintegrationsdienst die Eigenschaft „Abgelehnte IP-Adressen“ zum Bestimmen der Clients, die Anfragen senden können.</p>

Option	Beschreibung
HttpConfigurationOptions.DeniedHostNames	<p>Liste der Konstanten oder regulären Java-Expressionsmuster im Vergleich zu den Hostnamen des anfragenden Computers. Die Hostnamen unterliegen der Groß-/Kleinschreibung. Trennen Sie mehrere Konstanten oder Expressionen durch ein Leerzeichen.</p> <p>Wenn Sie diese Eigenschaft konfigurieren, nimmt der Datenintegrationsdienst Anfragen von Hosts an, deren Namen nicht mit dem Muster der abgelehnten Hostnamen übereinstimmen. Wenn Sie diese Eigenschaft nicht konfigurieren, verwendet der Datenintegrationsdienst die Eigenschaft „Zulässige Hostnamen“ zum Bestimmen der Clients, die Anfragen senden können.</p>
HttpConfigurationOptions.DeniedIPAddresses	<p>Liste der Konstanten oder regulären Java-Expressionsmuster im Vergleich zur IP-Adresse des anfragenden Computers. Trennen Sie mehrere Konstanten oder Expressionen durch ein Leerzeichen.</p> <p>Wenn Sie diese Eigenschaft konfigurieren, nimmt der Datenintegrationsdienst Anfragen von IP-Adressen an, die nicht mit dem Muster der abgelehnten IP-Adresse übereinstimmen. Wenn Sie diese Eigenschaft nicht konfigurieren, verwendet der Datenintegrationsdienst die Eigenschaft „Zulässige IP-Adressen“ zum Bestimmen der Clients, die Anfragen senden können.</p>
HttpConfigurationOptions.HTTPProtocolType	<p>Sicherheitsprotokoll, das vom Datenintegrationsdienst verwendet wird. Geben Sie einen der folgenden Werte ein:</p> <ul style="list-style-type: none"> <li>- HTTP. In Anfragen an den Dienst muss eine HTTP-URL verwendet werden..</li> <li>- HTTPS. In Anfragen an den Dienst muss eine HTTPS-URL verwendet werden.</li> <li>- Beide. In Anfragen an den Dienst kann entweder eine HTTP- oder eine HTTPS-URL verwendet werden.</li> </ul> <p>Wenn Sie den HTTP-Protokolltyp auf „HTTPS“ oder „Beide“ einstellen, aktivieren Sie TLS (Transport Layer Security) für den Dienst.</p> <p>Sie können TLS auch für jeden Webdienst aktivieren, der einer Anwendung bereitgestellt ist. Wenn Sie HTTPS für den Data Integration Service und TLS für den Webdienst aktivieren, verwendet der Webdienst eine HTTPS-URL. Wenn Sie HTTPS für den Data Integration Service und nicht für den Webdienst aktivieren, kann der Webdienst eine HTTP-URL oder eine HTTPS-URL nutzen. Wenn Sie TLS für einen Webdienst aktivieren, aber HTTPS nicht für den Data Integration Service aktivieren, startet der Webdienst nicht.</p> <p>Standardwert ist „HTTP“.</p>
HttpProxyServerOptions.HttpProxyServerDomain	Domäne für die Authentifizierung.
HttpProxyServerOptions.HttpProxyServerHost	Name des HTTP-Proxy-Servers.
HttpProxyServerOptions.HttpProxyServerPassword	Passwort für den authentifizierten Benutzer. Der Dienstmanager verschlüsselt das Passwort. Dies ist erforderlich, wenn der Proxy-Server Authentifizierung verlangt.
HttpProxyServerOptions.HttpProxyServerPort	Portnummer des HTTP-Proxy-Servers. Standardwert ist 8080.

Option	Beschreibung
HttpProxyServerOptions.HttpServerUser	Authentifizierter Benutzername für den HTTP-Proxy-Server. Dies ist erforderlich, wenn der Proxy-Server Authentifizierung verlangt.
LoggingOptions.LogLevel	Ebene der Fehlermeldungen, die der Datenintegrationsdienst in das Dienstprotokoll schreibt. Wählen Sie eine der folgenden Meldungsebenen aus: Fatal, Error, Warning, Info, Trace oder Debug.
MappingServiceOptions.MaxMemPerRequest	<p>Das Verhalten von „Maximale Speichergröße pro Anfrage“ richtet sich nach den folgenden Datenintegrationsdienst-Konfigurationen:</p> <ul style="list-style-type: none"> <li>- Der Dienst führt Jobs in lokalen Prozessen oder Remoteprozessen aus oder die Diensteigenschaft „Maximale Speichergröße“ lautet 0 (Standardeinstellung). In diesem Fall stellt „Maximale Speichergröße pro Anfrage“ die maximale Speichermenge in Byte dar, die der Datenintegrationsdienst allen Umwandlungen zuordnen kann, die den automatischen Cache-Modus in einer einzelnen Anfrage verwenden. Der Dienst weist Arbeitsspeicher separat zu Umwandlungen zu, die über eine bestimmte Cache-Größe verfügen. Der von der Anfrage verwendete Gesamtspeicher kann den Wert für „Maximale Speichergröße pro Anfrage“ überschreiten.</li> <li>- Der Dienst führt Jobs in dem Prozess des Datenintegrationsdiensts aus und die Diensteigenschaft „Maximale Speichergröße“ ist größer als 0. In diesem Fall stellt „Maximale Speichergröße pro Anfrage“ die maximale Speichermenge in Byte dar, die der Datenintegrationsdienst einer einzelnen Anfrage zuordnen kann. Der von der Anfrage verwendete Gesamtspeicher darf den Wert für „Maximale Speichergröße pro Anfrage“ nicht überschreiten.</li> </ul> <p>Standardwert ist 536.870.912.</p>
MappingServiceOptions.MaxNotificationThreadPoolSize	Weist die Anzahl an Threads zu, die Benachrichtigungen an den Client senden.
Modules.MappingService	Geben Sie FALSE ein, um das Modul zu deaktivieren, das Zuordnungen und Vorschauen ausführt. Standardwert ist „True“.
Modules.ProfilingService	Geben Sie FALSE ein, um das Modul zu deaktivieren, das Profile ausführt und Scorecards erzeugt. Standardwert ist „True“.
Modules.RESTService	Geben Sie „False“ ein, um das Modul zu deaktivieren, das den REST-Webdienst ausführt. Standardwert ist „True“.
Modules.SQLService	Geben Sie „False“ ein, um das Modul zu deaktivieren, das SQL-Abfragen in einem SQL-Datendienst ausführt. Standardwert ist „True“.
Modules.WebService	Geben Sie FALSE ein, um das Modul zu deaktivieren, das Webdienst-Vorgangszuordnungen ausführt. Standardwert ist „True“.
Modules.WorkflowOrchestrationService	Geben Sie FALSE ein, um das Modul zu deaktivieren, das Arbeitsabläufe ausführt. Standardwert ist „True“.

Option	Beschreibung
PassThroughSecurityOptions.AllowCaching	Ermöglicht Datenobjekt-Caching für alle Pass-Through-Verbindungen im Datenintegrationsdienst. Befüllt den Datenobjekt-Cache mithilfe der Anmeldedaten im Verbindungsobjekt. <b>Hinweis:</b> Wenn Sie Datenobjekt-Caching mit Pass-Through-Sicherheit aktivieren, lassen Sie unter Umständen nicht autorisierten Zugriff auf bestimmte Daten zu.
ProfilingServiceOptions.ExportPath	Speicherort zum Exportieren von Profilergebnissen. Geben Sie den Dateisystempfad ein. Standardwert ist „./ProfileExport“.
ProfilingServiceOptions.MaxExecutionConnections	Maximale Anzahl an Datenbankverbindungen für jeden Profiling-Job.
ProfilingServiceOptions.MaxPatterns	Maximale Anzahl der für ein Profil anzuzeigenden Muster
ProfilingServiceOptions.MaxProfileExecutionPoolSize	Maximale Anzahl an Threads zum Ausführen des Profiling.
ProfilingServiceOptions.MaxRanks	Anzahl der Höchst- und Minimalwerte, die für ein Profil angezeigt werden sollen. Standardwert ist 5. Standardwert ist 10.
ProfilingServiceOptions.ProfileWarehouseConnectionName	Name des Verbindungsobjekts für die Verbindung mit dem Profiling Warehouse.
RepositoryOptions.RepositoryPassword	Benutzerpasswort für den Zugriff auf das Modellrepository.
RepositoryOptions.RepositorySecurityDomain	Name der LDAP-Sicherheitsdomäne, wenn Sie LDAP verwenden. Wenn Sie LDAP nicht verwenden, ist die Standarddomäne nativ.
RepositoryOptions.RepositoryServiceName	Dienst, der Laufzeitmetadaten speichert, die zur Ausführung von Zuordnungen und SQL-Datendiensten erforderlich sind.
RepositoryOptions.RepositoryUserName	Benutzername für den Zugriff auf das Modellrepository. Der Benutzer muss über die Berechtigung zum Erstellen von Projekten für den Modellrepository-Dienst verfügen.
ResultSetCacheOptions.EnableEncryption	Gibt an, ob die Ergebnissatz-Cachedateien mit der 128-Bit-AES-Verschlüsselung verschlüsselt werden. Gültige Werte sind „True“ oder „False“. Standardwert ist „True“.
ResultSetCacheOptions.FileNamePrefix	Das Präfix für die Namen aller Ergebnissatz-Cachedateien, die auf dem Datenträger gespeichert sind. Standardwert ist RSCACHE.

Option	Beschreibung
SQLServiceOptions.DTMKeepAliveTime	<p>Anzahl an Millisekunden, die der DTM-Prozess geöffnet bleibt, nachdem er die letzte Anfrage abgeschlossen hat. Identische SQL-Abfragen können den offenen Prozess wiederverwenden.</p> <p>Verwenden Sie die Keep Alive-Zeit, um die Leistung zu erhöhen, wenn die für die Verarbeitung der SQL-Abfrage erforderliche Zeit im Vergleich zur Dauer der Initialisierung des DTM-Prozesses gering ist. Wenn die Abfrage fehlschlägt, wird der DTM-Prozess beendet. Muss größer oder gleich 0 sein. 0 bedeutet, dass der Datenintegrationsdienst den DTM-Prozess nicht im Speicher beibehält. Standardwert ist 0.</p> <p>Sie können diese Eigenschaft auch für jeden SQL-Datendienst festlegen, der auf dem Datenintegrationsdienst bereitgestellt wird. Wenn Sie diese Eigenschaft für einen bereitgestellten SQL-Datendienst festlegen, überschreibt der Wert für den bereitgestellten SQL-Datendienst den Wert, den Sie für den Datenintegrationsdienst festgelegt haben.</p>
SQLServiceOptions.MaxMemPerRequest	<p>Das Verhalten von „Maximale Speichergröße pro Anfrage“ richtet sich nach den folgenden Datenintegrationsdienst-Konfigurationen:</p> <ul style="list-style-type: none"> <li>- Der Dienst führt Jobs in lokalen Prozessen oder Remoteprozessen aus oder die Diensteigenschaft „Maximale Speichergröße“ lautet 0 (Standardeinstellung). In diesem Fall stellt „Maximale Speichergröße pro Anfrage“ die maximale Speichermenge in Byte dar, die der Datenintegrationsdienst allen Umwandlungen zuordnen kann, die den automatischen Cache-Modus in einer einzelnen Anfrage verwenden. Der Dienst weist Arbeitsspeicher separat zu Umwandlungen zu, die über eine bestimmte Cache-Größe verfügen. Der von der Anfrage verwendete Gesamtspeicher kann den Wert für „Maximale Speichergröße pro Anfrage“ überschreiten.</li> <li>- Der Dienst führt Jobs in dem Prozess des Datenintegrationsdiensts aus und die Diensteigenschaft „Maximale Speichergröße“ ist größer als 0. In diesem Fall stellt „Maximale Speichergröße pro Anfrage“ die maximale Speichermenge in Byte dar, die der Datenintegrationsdienst einer einzelnen Anfrage zuordnen kann. Der von der Anfrage verwendete Gesamtspeicher darf den Wert für „Maximale Speichergröße pro Anfrage“ nicht überschreiten.</li> </ul> <p>Standardwert ist 50.000.000.</p>
SQLServiceOptions.SkipLogFiles	<p>Hindert den Datenintegrationsdienst daran, Protokolldateien zu erstellen, wenn die SQL-Datendienstanfrage erfolgreich abgeschlossen wird und die Tracing-Ebene auf INFO oder höher festgelegt ist. Standardwert ist „false“.</p>
SQLServiceOptions.TableStorageConnection	<p>Relationale Datenbankverbindung, die temporäre Tabellen für SQL-Datendienste speichert. Standardmäßig ist keine Verbindung ausgewählt.</p>
WorkflowOrchestrationServiceOptions.DBName	<p>Verbindungsname der Datenbank, in der Laufzeitmetadaten für Arbeitsabläufe gespeichert werden.</p>

Option	Beschreibung
WorkflowOrchestrationServiceOptions.MaxWorkerThreads	<p>Die maximale Anzahl an Threads, die vom Datenintegrationsdienst verwendet werden können, um parallele Aufgaben zwischen einem Paar inklusiver Gateways in einem Arbeitsablauf auszuführen. Der Standardwert ist 10.</p> <p>Wenn die Anzahl der Aufgaben zwischen den inklusiven Gateways größer als der Maximalwert ist, führt der Datenintegrationsdienst die Aufgaben in vom Wert angegebenen Batches aus. Wenn der Wert für die maximale Anzahl an Worker-Threads beispielsweise auf 10 festgelegt wurde, führt der Datenintegrationsdienst die Aufgaben in Batches zu je zehn Blöcken aus.</p>
WSServiceOptions.DTMKeepAliveTime	<p>Anzahl an Millisekunden, die der DTM-Prozess geöffnet bleibt, nachdem er die letzte Anfrage abgeschlossen hat. Webdienst-Anfragen für dieselbe Operation können den offenen Prozess wiederverwenden.</p> <p>Verwenden Sie die Keep Alive-Zeit, um die Leistung zu erhöhen, wenn die für die Verarbeitung der Anfrage erforderliche Zeit im Vergleich zur Dauer der Initialisierung des DTM-Prozesses gering ist. Wenn die Anfrage fehlschlägt, wird der DTM-Prozess beendet. Muss größer oder gleich 0 sein. 0 bedeutet, dass der Datenintegrationsdienst den DTM-Prozess nicht im Speicher beibehält. Standardwert ist 5000.</p> <p>Sie können diese Eigenschaft auch für jeden Webdienst festlegen, der auf dem Datenintegrationsdienst bereitgestellt wird. Wenn Sie diese Eigenschaft für einen bereitgestellten Webdienst festlegen, überschreibt der Wert für den bereitgestellten Webdienst den Wert, den Sie für den Datenintegrationsdienst festgelegt haben.</p>
WSServiceOptions.MaxMemPerRequest	<p>Das Verhalten von „Maximale Speichergröße pro Anfrage“ richtet sich nach den folgenden Datenintegrationsdienst-Konfigurationen:</p> <ul style="list-style-type: none"> <li>- Der Dienst führt Jobs in lokalen Prozessen oder Remoteprozessen aus oder die Diensteigenschaft „Maximale Speichergröße“ lautet 0 (Standardeinstellung). In diesem Fall stellt „Maximale Speichergröße pro Anfrage“ die maximale Speichermenge in Byte dar, die der Datenintegrationsdienst allen Umwandlungen zuordnen kann, die den automatischen Cache-Modus in einer einzelnen Anfrage verwenden. Der Dienst weist Arbeitsspeicher separat zu Umwandlungen zu, die über eine bestimmte Cache-Größe verfügen. Der von der Anfrage verwendete Gesamtspeicher kann den Wert für „Maximale Speichergröße pro Anfrage“ überschreiten.</li> <li>- Der Dienst führt Jobs in dem Prozess des Datenintegrationsdiensts aus und die Diensteigenschaft „Maximale Speichergröße“ ist größer als 0. In diesem Fall stellt „Maximale Speichergröße pro Anfrage“ die maximale Speichermenge in Byte dar, die der Datenintegrationsdienst einer einzelnen Anfrage zuordnen kann. Der von der Anfrage verwendete Gesamtspeicher darf den Wert für „Maximale Speichergröße pro Anfrage“ nicht überschreiten.</li> </ul> <p>Standardwert ist 50.000.000.</p>



Option	Beschreibung
WSServiceOptions.SkipLogFiles	Hindert den Datenintegrationsdienst daran, Protokolldateien zu erstellen, wenn die Webdienstanfrage erfolgreich abgeschlossen wird und die Tracing-Ebene auf INFO oder höher festgelegt ist. Standardwert ist „False“.
WSServiceOptions.WSDLLogicalURL	Präfix für die WSDL-URL, wenn Sie einen externen HTTP-Load Balancer verwenden. Beispiel: http://loadbalancer:8080  Der Datenintegrationsdienst benötigt einen externen HTTP-Load Balancer, um einen Webdienst auf einem Gitter auszuführen. Wenn Sie den Datenintegrationsdienst auf einem Einzelknoten ausführen, müssen Sie keine logische URL angeben.

## UpdateServiceProcessOptions

Aktualisiert Eigenschaften für einen Datenintegrationsdienst-Prozess. Führen Sie zum Anzeigen der aktuellen Eigenschaften den `infacmd` `dis ListServiceProcessOptions`-Befehl aus.

Geben Sie die Optionen in folgendem Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Der Befehl „`infacmd` `dis UpdateServiceProcessOptions`“ verwendet die folgende Syntax:

```
UpdateServiceProcessOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis UpdateServiceProcessOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
NodeName -nn	node_name	Erforderlich. Knoten, auf dem der Datenintegrationsdienst ausgeführt wird.
-Options -o	options	Erforderlich. Geben Sie jede Option durch ein Leerzeichen getrennt ein. Führen Sie zum Anzeigen der Optionen den infacmd dis ListServiceProcessOptions-Befehl aus.

## Prozessoptionen des Datenintegrationsdiensts

Verwenden Sie die Prozessoptionen des Datenintegrationsdiensts mit dem infacmd dis UpdateServiceProcessOptions-Befehl.

Geben Sie die Prozessoptionen des Datenintegrationsdiensts in folgendem Format ein:

- Trennen Sie mehrere Optionen mit einem Leerzeichen.
- Schließen Sie alle Optionen und Werte in doppelte Anführungszeichen ein.
- Schließen Sie Parameter in einfache Anführungszeichen ein.

```
... -o "option_type.option_name='value'"
```

In der folgenden Tabelle werden die Prozessoptionen des Datenintegrationsdiensts beschrieben:

Option	Beschreibung
GeneralOptions.JVMOptions	Java Virtual Machine (JVM)-Befehlszeilenoptionen zum Ausführen von Java-basierten Programmen. Bei der Konfiguration von JVM-Optionen müssen Sie die Eigenschaften für den Java SDK-Klassenpfad, den Java SDK-Minimalspeicher und den Java SDK-Maximalspeicher festlegen.
GeneralOptions.HttpPort	Eindeutige HTTP-Portnummer für den Datenintegrationsdienstprozess, wenn der Dienst das HTTP-Protokoll verwendet.
GeneralOptions.HttpsPort	Eindeutige HTTPS-Portnummer für den Datenintegrationsdienstprozess, wenn der Dienst das HTTPS-Protokoll verwendet.

Option	Beschreibung
LoggingOptions.LogDirectory	<p>Verzeichnis der Knotenprozessprotokolle des Datenintegrationsdiensts. Standardwert ist &lt;INFA_HOME&gt;\logs\dislogs.</p> <p>Wenn der Datenintegrationsdienst in einem Gitter ausgeführt wird, verwenden Sie zum Erstellen eines Verzeichnisses für Protokolldateien ein gemeinsam genutztes Verzeichnis. Durch ein gemeinsam genutztes Verzeichnis stellen Sie sicher, dass bei einem Failover des Master-Dienstprozesses auf einen anderen Knoten der neue Master-Dienstprozess auf frühere Protokolldateien zugreifen kann.</p>
ResultSetCacheOptions.MaxTotalDiskSize	Maximale Byte-Anzahl, die für den Dateispeicher des Ergebnissatz-Caches zulässig ist. Standardwert ist 0.
ResultSetCacheOptions.MaxPerCacheMemorySize	Maximale Byte-Anzahl, die einer einzelnen Ergebnissatz-Cache-Instanz im Arbeitsspeicher zugewiesen ist. Standardwert ist 0.
ResultSetCacheOptions.MaxTotalMemorySize	Maximale Byte-Anzahl, die dem Speicher des Ergebnissatz-Caches im Arbeitsspeicher insgesamt zugewiesen ist. Standardwert ist 0.
ResultSetCacheOptions.MaxNumCaches	Maximale Anzahl an Ergebnissatz-Cache-Instanzen, die für diesen Datenintegrationsdienstprozess zulässig sind. Standardwert ist 0.
HttpConfigurationOptions.MaxConcurrentRequests	Anzahl der HTTP- oder HTTPS-Verbindungen, die zu diesem Datenintegrationsdienst-Prozess hergestellt werden können. Der Minimalwert ist 4. Standardwert ist 200.
HttpConfigurationOptions.MaxBacklogRequests	Anzahl der HTTP- oder HTTPS-Verbindungen, die in der Warteschlange für diesen Datenintegrationsdienst-Prozess warten können. Standardwert ist 100.
HttpConfigurationOptions.KeyStoreFile	<p>Pfad und Dateiname der Schlüsselspeicherdatei, die die Schlüssel und Zertifikate enthält, die zur Verwendung des HTTPS-Protokolls für den Datenintegrationsdienst erforderlich sind. Sie können eine Schlüsselspeicherdatei mit einem Keytool erstellen. Bei Keytool handelt es sich um ein Dienstprogramm, das private oder öffentliche Schlüsselpaare und zugeordnete Zertifikate in einer Schlüsselspeicherdatei erzeugt und speichert. Sie können das selbstsignierte Zertifikat nutzen oder ein Zertifikat verwenden, das von einer Zertifizierungsstelle signiert wurde.</p> <p>Wenn Sie den Datenintegrationsdienst in einem Gitter ausführen, muss die Schlüsselspeicherdatei auf jedem Knoten im Gitter die gleichen Schlüssel enthalten.</p>
HttpConfigurationOptions.KeyStorePassword	Passwort für die Schlüsselspeicherdatei.
HttpConfigurationOptions.TrustStoreFile	<p>Pfad und Dateiname der Truststore-Datei, die Authentifizierungszertifikate enthält, die vom Datenintegrationsdienst als vertrauenswürdig eingestuft werden.</p> <p>Wenn Sie den Datenintegrationsdienst in einem Gitter ausführen, muss die Truststore-Datei auf jedem Knoten im Gitter die gleichen Schlüssel enthalten.</p>

Option	Beschreibung
HttpConfigurationOptions.TrustStorePassword	Passwort für die Truststore-Datei.
HttpConfigurationOptions.SSLProtocol	Zu verwendendes Secure Sockets Layer-Protokoll. Standardwert ist TLS.
SQLServiceOptions.MaxConcurrentConnections	Begrenzt die Anzahl der Datenbankverbindungen, die der Datenintegrationsdienst für SQL-Datendienste herstellen kann. Standardwert ist 100.

## Regeln und Richtlinien

Im Folgenden finden Sie die Regeln und Richtlinien für die Verwendung der infacmd dis-Befehle.

Beachten Sie die folgenden Regeln und Richtlinien, wenn Sie die infacmd dis-Befehle verwenden:

### Allgemeine Regeln und Richtlinien

- Das Zeitzoneattribut akzeptiert nur Werte von java.time.ZoneID(). Beispielsweise wird IST nicht unterstützt.
- Passwörter, die mit dem Dienstprogramm „pmpasswd“ verschlüsselt sind, müssen mit der Option -e=CRYPT\_SYSTEM verschlüsselt werden.
- Sie benötigen Leseberechtigungen für ein Objekt, um es abzufragen.
- Sie können keine gelöschten Objekte abfragen, selbst wenn die gelöschten Objekte Teil einer ausstehenden Änderungsliste eines Modellrepositorys sind, das in ein Versionsverwaltungssystem integriert ist.
- Wenn Sie zwei Zuordnungen vergleichen, wird im Vergleichsbericht ein Leerzeichen gedruckt.
- Wenn Sie zwei Zuordnungen vergleichen und Blaze als Ausführungsumgebung verwenden, wird im Vergleichsbericht die Engine CADIYarnExecutionEngine anstelle von Blaze angezeigt.

### Regeln und Richtlinien für Anwendungs-Patches

- Wenn Sie in einer Anwendungs-Patch-Archivdatei Objekte bereitstellen, ist der Standardspeicherort der Datei \$INFA\_HOME/tomcat/bin/target. Wenn der Datenintegrationsdienst für die Verwendung der Betriebssystemprofile konfiguriert ist und Sie das Betriebssystemprofil angeben, wird die Archivdatei stattdessen in \$DISTargetDir gespeichert.

# KAPITEL 14

## Infacmd dis-Abfragen

Dieses Kapitel umfasst die folgenden Themen:

- [Abfragen, 290](#)
- [Vergleichsoperatoren, 291](#)
- [Logische Operatoren, 293](#)
- [Abfrageparameter, 293](#)
- [Abfragestruktur, 295](#)
- [Where-Klausel, 295](#)

## Abfragen

Verwenden Sie Abfragen, um Entwurfs- und Laufzeitobjekte abzurufen.

Sie können Entwurfszeitobjekte aus einem Modellrepository oder Laufzeitobjekte abrufen, die einem Datenintegrationsdienst bereitgestellt wurden. Verwenden Sie zum Erstellen einer Abfrage Abfrageparameter, die die abzurufenden Objekte angeben. Sie können eine Abfrage weiter verfeinern, indem Sie die Where-Klausel und Operatoren verwenden.

Die folgenden Befehle akzeptieren eine Abfrage als Befehlszeilenoption:

- `compareMapping`
- `deployObjectsToFile`
- `queryRunTimeObjects`
- `queryDesignTimeObjects`
- `replaceAllTag`
- `Tag`
- `untag`

Wenn Sie eine Abfrage an einen Befehl übergeben, wird der Befehl nur auf die Objekte angewendet, die die Abfrage zurückgibt. Wenn Sie die Abfrage `name=mapping1` an den Befehl „`infacmd dis tag`“ übergeben, weist der Befehl Tags nur Objekten zu, die den Namen `mapping1` haben.

Um eine Abfrage an die Befehle zu übergeben, geben Sie die Abfrage als Zeichenfolge an. Beachten Sie z. B. den Wert für die Option -q in der Befehlssyntax für den folgenden Befehl „infacmd dis queryDesignTimeObjects“:

```
./infacmd.sh dis queryDesignTimeObjects -dn Domain_v299 -un Administrator
-pd Administrator -rs MRS_v299 -rsun Administrator -rspd Administrator
-q "all" -sn DIS_v299
```

## Vergleichsoperatoren

Verwenden Sie die Vergleichsoperatoren mit Abfrageparametern, um eine Abfrage zu erstellen. Sie können Vergleichsoperatoren verwenden, um beim Abfragen von Objekten Kriterien anzugeben.

In der folgenden Tabelle werden die Vergleichsoperatoren aufgelistet, die Sie mit jedem Abfrageparametertyp verwenden können:

Typ des Abfrageparameters	Enthält Abfrageparameter	Vergleichsoperatoren	Beispiele
Subjekt	name Tag createdBy lastModifiedBy	~contains~ ~not-contains~ ~not-ends-with~ ~not-starts-with~ ~ends-with~ ~starts-with~ = != ~in~ ~not-in~	Name ~contains~ Zuordnung Tag ~in~ (tg_1, tg_2, tg_3) createdBy = Administrator lastModifiedBy ~ends-with~ Besucher
Betreff	object type	= != ~in~ ~not-in~	type = Mapping object != Mapping object <sub>in</sub> (P1/F1/Map1,P2/F1/Map2)
Uhrzeit	lastModifiedTime checkInTime checkOutTime creationTime	> < ~within-last~ ~between~ ~not-between~	lastModifiedTime < 2019-02-26 20:32:54 checkInTime ~between~ (2018-12-26 20:32:54, 2018-05-26 20:32:54) checkOutTime ~within-last~ 10 (Tage)

Typ des Abfrageparameters	Enthält Abfrageparameter	Vergleichsoperatoren	Beispiele
Status	versionStatus	~is-checkedin~ ~is-checkedout~	versionStatus ~is-checkedin~ versionStatus ~is-checkedout~
Speicherort	Ordner Projekt Anwendung	~contains~ ~not-ends-with~ ~not-contains~ ~not-starts-with~ ~ends-with~ ~starts-with~ = != ~in~ ~not-in~	name ~contains~ Mapping where project ~ends-with~ _1 lastModifiedBy ~ends-with~ trator where folder ~not-in~ (Folder_3, Folder_2) all where project=Project_1, folder=Folder_1 name = Mapping where project=Project_1, folder=/Folder_1/ Folder_2/ name = Mapping where project=Project_1, folder=/ name = captain_america where app~in~ (MapGenTest, MapGenEg)

Wenn Sie eine Abfrage durch Angabe eines Kriteriums mithilfe von Vergleichsoperatoren erstellt haben, gibt die Abfrage das Objekt an den Client zurück, der das Kriterium erfüllt.

Sie können beispielsweise eine Abfrage zum Abrufen von Objekten erstellen, die den Namen `mapping 1` aufweisen.

```
name=mapping1
```

**Hinweis:** Das Zeitformat ist YYYY-MM-DD HH24:MI:SS.

## Angabe eines Ordnerpfads

Verwenden Sie zum Erstellen einer Abfrage einen rekursiven oder nicht rekursiven Ordnerpfad. Sie können den Ordnerpfad angeben, um auf Objekte innerhalb eines Ordners zuzugreifen.

Sie können die folgenden Typen von Ordnerpfaden verwenden:

- Rekursiv. Enthält Objekte im Ordner und allen Unterordnern.
- Nicht rekursiv. Enthält nur die Objekte innerhalb des Root-Ordners.

Ordnerpfade sind standardmäßig rekursiv. Zur Angabe eines nicht rekursiven Ordnerpfads verwenden Sie einen Schrägstrich am Ende des Ordnerpfads.

In der folgenden Tabelle werden Beispielabfragen mit rekursiven und nicht rekursiven Ordnerpfaden beschrieben:

Beispielabfrage	Beschreibung
name=map1 folder=/ 	Nicht rekursiv. Die Abfrage untersucht nur die Objekte, die sich direkt unter dem Projekt befinden.
name=map1 folder=/f1/f2/ 	Nicht rekursiv. Die Abfrage untersucht nur die Objekte, die sich im Pfad /f1/f2/ befinden.



Beispielabfrage	Beschreibung
name=map1 folder=f1	Rekursiv. Die Abfrage untersucht alle Objekte, die sich im Ordner f1 und in allen Unterordnern von f1 befinden.
name=map1 folder=/f1/f2	Rekursiv. Die Abfrage untersucht alle Objekte, die sich im Pfad /f1/f2 und in allen Unterordnern von f2 befinden.

**Hinweis:** Wenn Sie einen Schrägstrich zur Angabe eines Ordnerpfads verwenden, stehen nur die folgenden Vergleichsoperatoren zur Verfügung: =, !=, ~in~ und ~not-in~.

## Logische Operatoren

Verwenden Sie logische Operatoren, um zu testen, ob eine oder mehrere Bedingungen in einer Abfrage TRUE oder FALSE sind.

Sie können folgende logische Operatoren verwenden:

Logischer Operator	Beschreibung	Beispiel
!	NOT	! Name ~not-starts-with~ M_
&&	AND	Name ~starts-with~ map_&& lastModifiedBy ~ends-with~ Besucher
	OR	checkInTime > 2018-12-26 20:32:54    lastModifiedTime > 2019-02-26 20:32:54

**Hinweis:** Sie können keine logischen Operatoren verwenden, um Speicherortabfrageparameter, einschließlich Ordernamen, Projektnamen und Anwendungsamen, zu testen.

## Abfrageparameter

Verwenden Sie Abfrageparameter, um Entwurfszeitobjekte in einem Modellrepository und Laufzeitobjekte abzufragen, die in einem Datenintegrationsdienst bereitgestellt werden. Sie können das Subjekt, die Uhrzeit, den Status und den Speicherort zum Erstellen einer Abfrage verwenden.

Abfrageparameter werden in folgende Parametertypen unterteilt:

## Subjekt

Parameter, die ein Subjekt testen, wie z. B. ein bestimmtes Objekt oder einen bestimmten Benutzer. In der folgenden Tabelle werden die Parameter für Subjekte aufgelistet:

Parameter	Objekttyp	Beschreibung
name	Entwurfszeitobjekt Laufzeitobjekt	Name des Objekts, das Sie abfragen möchten. Sie können den Namen eines der folgenden Objekttypen angeben: <ul style="list-style-type: none"><li>- Mapping</li><li>- Physisches Datenobjekt</li><li>- Parametersatz</li></ul>
Tag	Entwurfszeitobjekt	Tag, das dem Objekt zugewiesen ist.
createdBy	Entwurfszeitobjekt	Benutzer, der das Objekt erstellt hat.
lastModifiedBy	Entwurfszeitobjekt	Benutzer, der das Objekt zuletzt geändert hat.
Typ	Entwurfszeitobjekt	Filtert den Objekttyp.
object	Entwurfszeitobjekt	Filtert und ruft Objekte aus einem Ordner ab. Geben Sie den vollständigen Pfad zu Objekten ab Root an, einschließlich des Projektnamens, der Ordner und des Objektnamens.

## Uhrzeit

Parameter, die die Uhrzeit testen, zu der ein Objekt geändert wurde. In der folgenden Tabelle werden die Parameter für Uhrzeiten aufgelistet:

Parameter	Objekttyp	Beschreibung
lastModifiedTime	Entwurfszeitobjekt	Zeitpunkt, zu dem das Objekt zuletzt geändert wurde.
checkInTime	Entwurfszeitobjekt	Zeitpunkt, zu dem das Objekt zuletzt eingecheckt wurde. <b>Hinweis:</b> Gilt nur, wenn ein Versionsverwaltungssystem im Modellrepository integriert ist.
checkOutTime	Entwurfszeitobjekt	Zeitpunkt, zu dem das Objekt zuletzt ausgecheckt wurde. <b>Hinweis:</b> Gilt nur, wenn ein Versionsverwaltungssystem im Modellrepository integriert ist.
creationTime	Entwurfszeitobjekt	Zeitpunkt, zu dem das Objekt erstellt wurde.

## Status

Parameter, die den Status eines Objekts testen. In der folgenden Tabelle werden die Parameter für Statusangaben aufgelistet:

Parameter	Objekttyp	Beschreibung
versionStatus	Entwurfszeitobjekt	Versionsstatus des Objekts. Der Versionsstatus kann entweder eingecheckt oder ausgecheckt lauten. <b>Hinweis:</b> Gilt nur, wenn ein Versionsverwaltungssystem im Modellrepository integriert ist.

### Speicherort

Parameter, die den Speicherort eines Objekts testen, wie z. B. eines bestimmten Projekts, eines Ordners oder einer Laufzeitanwendung. In der folgenden Tabelle werden die Parameter für Speicherorte aufgelistet:

Parameter	Objekttyp	Beschreibung
Ordner	Entwurfszeitobjekt	Ordner, der das Objekt enthält.
Projekt	Entwurfszeitobjekt	Projekt, das das Objekt enthält.
Anwendung	Laufzeitobjekt	Name der Laufzeitanwendung, die das Objekt enthält.

## Abfragestruktur

Verwenden Sie zum Erstellen einer Abfrage Parameter, Vorgänge und die Where-Klausel.

Sie können eine Abfrage strukturieren, indem Sie Parameter, Vergleichsoperatoren, logische Operatoren und die Where-Klausel verwenden. Sie können den Vorrang von Abfragen mithilfe von Klammern steuern.

Eine Abfrage kann mit den folgenden Elementen strukturiert werden:

### Abfrageparameter

Abfrageparameter werden in Subjekt, Uhrzeit, Status und Speicherort kategorisiert. Jeder Abfrageparameter muss einen Vergleichsoperator enthalten. Beispiel:

```
type = mapping
```

### Vergleichsoperatoren

Vergleichsoperatoren werden verwendet, um Kriterien für die Abfrage von Objekten anzugeben. Vergleichsoperatoren werden zusammen mit den Abfrageparametern verwendet, um eine Abfrage zu erstellen.

### Logische Operatoren

Logische Operatoren werden verwendet, um eine Bedingung in einer Abfrage zu testen. Logische Operatoren können mehrere Abfrageparameter haben. Beispiel:

```
type = mapping || createdBy = admin
```

### Where-Klausel

Die Where-Klausel dient dazu, den Abfrageumfang einzuschränken. Beispiel:

```
name = mapping1 where project = project1, folder = folder1.
```

## Where-Klausel

Verwenden Sie eine Where-Klausel, um den Umfang einer Abfrage einzuschränken.

Sie können innerhalb einer Where-Klausel nur Speicherortabfrageparameter angeben. Da Parameter zur Speicherortabfrage keine Unterstützung für logische Operatoren bieten, können logische Operatoren nicht innerhalb der Where-Klausel verwendet werden.

Beispielsweise findet die folgende Abfrage eine Zuordnung innerhalb eines bestimmten Projekts und Ordners:

```
name=mapping1 where project1, folder=folder1
```

Sie können außerhalb der Where-Klausel Klammern verwenden. Die folgende Abfrage verwendet beispielsweise die Ausdrücke `(name contains super && name ends-with boy)` und `(name contains ragnarok)`, die in Klammern eingeschlossen sind und sich außerhalb der Where-Klausel befinden:

```
(name contains super && name ends-with boy) || (name contains ragnarok) where  
project=MapGenTest
```

Sie können das Schlüsselwort `all` zum Auffinden aller Entwurfszeitobjekte in einem Modellrepository oder aller Laufzeitobjekte verwenden, die in einem Datenintegrationsdienst bereitgestellt werden. Sie können das Schlüsselwort `all` mit der Where-Klausel verwenden.

Beispielsweise findet die folgende Abfrage alle Objekte innerhalb eines bestimmten Ordners:

```
all where folder=Folder_1
```

## KAPITEL 15

# infacmd dp-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [startSparkJobServer, 297](#)
- [stopSparkJobServer, 299](#)

## startSparkJobServer

Startet den Spark-Jobserver auf dem Computer des Datenintegrationsdiensts. Der Spark-Jobserver wird standardmäßig gestartet, wenn Sie hierarchische Daten in der Vorschau anzeigen.

Führen Sie diesen Befehl zum manuellen Starten des Spark-Jobservers im Hintergrund aus, um bei der Vorschau hierarchischer Daten Zeit zu sparen.

Der Befehl „infacmd dp startSparkJobServer“ verwendet die folgende Syntax:

```
startSparkJobServer
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-ConfigurationName|-cn> configuration_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dp startSparkJobServer“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariablen INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit diesen beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts.
-ConfigurationName -cn	Konfigurationsname	Erforderlich. Name der Cluster-Konfiguration

## stopSparkJobServer

Stoppt den auf dem angegebenen Datenintegrationsdienst ausgeführten Spark-Jobserver. Standardmäßig wird der Spark-Jobserver angehalten, wenn er 60 Minuten im Leerlauf ausgeführt wird oder wenn der Datenintegrationsdienst angehalten oder wiederhergestellt wird.

Der Befehl „infacmd dp startSparkJobServer“ verwendet die folgende Syntax:

```
startSparkJobServer
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dp stopSparkJobServer“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.



Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariablen INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit diesen beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts.

## KAPITEL 16

# infacmd idp-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [createRepository, 302](#)
- [createService, 304](#)
- [updateService, 309](#)
- [upgradeRepository, 312](#)

## createRepository

Creates a Data Preparation repository.

The infacmd idp createRepository command uses the following syntax:

```
createRepository  
  
<-DomainName|-dn> domain_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-SecurityDomain|-sdn> security_domain]  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]  
  
<-ServiceName|-sn> service_name
```

The following table describes infacmd idp createRepository options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.  If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Interactive Data Preparation Service associated with the Data Preparation repository.

## createService

Creates an Interactive Data Preparation Service.

The infacmd idp createService command uses the following syntax:

```
createService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name | <-GridName|-gn> grid_name

[<-BackupNodes|-bn> node_name1,node_name2,...]

<-ServiceOptions|-so> option_name=value ...
(HDFSConnection*,HiveConnection*,HadoopConnection*,HDFSSystemDirectory*,HiveTableStorageFormat(DefaultFormat|Parquet|ORC (default DefaultFormat)),LogLevel(FATAL|ERROR|WARNING|INFO|TRACE|DEBUG (default INFO)),customLogDirectory,SecurityMode(simple|kerberos (default simple)),KerberosPrincipal(Principal Name for User Impersonation),KerberosKeyTabFileName(SPN Keytab File for User Impersonation),LogAuditEvents(true|false (default false)),JDBCPort,ZeppelinURL,MaxFileUploadSize(default=512MB),DownloadRowsSize(default=100000),MaxRecommendations(default=10),MaxSampleSize(default=50000),SampleSize(default=50000),hiveExecutionEngine(MR|Spark|Tez|Cluster-Default (default=Cluster-Default)),LocalSystemDirectory*,SolrJVMOptions,IndexDir)

[<-LicenseName|-ln> license_name]

<-RepositoryServiceName |-rs> repository_service_name

<-RepositoryUser|-rsun> repository_user

[<-RepositoryPassword|-rspd> repository_password]

[<-RepositorySecurityDomain|-rssdn> model_repository_security_domain]
```

```

<-DISServiceName|-dsn> dis_service_name

<<-HttpPort|-hp> http_port|<-HttpsPort|-hsp> https_port>

[<-KeystoreFile|-kf> keystore_file_location]

[<-KeystorePassword|-kp> keystore_password]

[<-TruststoreFile|-tsf> truststore_file_location]

[<-TruststorePassword|-tsp> truststore_password]

[<-RulesServerPort|-rpo> RulesServerPort]

[<-SolrPort|-spo> SolrPort]

<-maxHeapSize|-mxhs> maxHeapSize]

[<-FolderPath|-fp> full_folder_path]

```

The following table describes infacmd idp createService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Interactive Data Preparation Service.  You cannot change the name of the service after you create it. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < >   ! ( ) [
-NodeName -nn	node_name	Required if you do not specify grid name. Node where the service runs.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.

Option	Argument	Description
-ServiceOptions -so	option_name=value ...	Optional. Service properties that define how the service runs. To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks. You can define the following available service options: <ul style="list-style-type: none"> <li>- HDFSCollection*</li> <li>- HiveConnection*</li> <li>- HadoopConnection*</li> <li>- HDFSSystemDirectory*</li> <li>- HiveTableStorageFormat(DefaultFormat Parquet ORC (default DefaultFormat))</li> <li>- LogLevel(FATAL ERROR WARNING INFO TRACE DEBUG (default INFO))</li> <li>- customLogDirectory</li> <li>- SecurityMode(simple kerberos (default simple))</li> <li>- KerberosPrincipal(Principal Name for User Impersonation)</li> <li>- KerberosKeyTabFileName(SPN Keytab File for User Impersonation)</li> <li>- LogAuditEvents(true false (default false))</li> <li>- JDBCPort</li> <li>- ZeppelinURL</li> <li>- MaxFileUploadSize(default=512MB)</li> <li>- DownloadRowsSize(default=1000000)</li> <li>- MaxRecommendations(default=10)</li> <li>- MaxSampleSize(default=50000)</li> <li>- SampleSize(default=50000)</li> <li>- hiveExecutionEngine(MR Spark Tez Cluster-Default (default=Cluster-Default))</li> <li>- LocalSystemDirectory*</li> <li>- SolrJVMOptions</li> <li>- IndexDir</li> </ul>
-LicenseName -ln	license_name	Optional. License object that allows the use of the service.
-RepositoryServiceName -rs	repository_service_name	Optional. Name of the Model Repository Service that manages the Model repository that contains rule objects and metadata. Set this property if rules are used during data preparation.
-RepositoryUser -rsun	-repository_username	Optional. User account to use to log in to the Model Repository Service.
-RepositoryPassword -rspd	-repository_password	Optional. Password for the Model Repository Service user account.
-RepositorySecurityDomain -rssdn	model_repository_security_domain	Optional. Security domain to which the Model Repository Service user account belongs.

Option	Argument	Description
-DISServiceName -dsn	dis_service_name	Optional. Name of the Data Integration Service that runs rules during data preparation. Set this property if rules are used during data preparation.
-HttpPort -hp	http_port	Required if you do not specify an HTTPS port. Unique HTTP port number used for each Data Integration Service process. After you create the service, you can define different port numbers for each service process.
-HttpsPort -hsp	https_port	Required if you do not specify an HTTP port. Unique HTTPS port number used for each Data Integration Service process. After you create the service, you can define different port numbers for each service process.
-KeystoreFile -kf	keystore_file_location	Optional. Path and file name of the keystore file that contains the keys and certificates required if you use the HTTPS protocol for the service. You can create a keystore file with a keytool. keytool is a utility that generates and stores private or public key pairs and associated certificates in a keystore file. You can use the self-signed certificate or use a certificate signed by a certificate authority.
-KeystorePassword -kp	keystore_password	Optional. Password for the keystore file.
-TruststoreFile -tsf	truststore_file_location	Optional. Path and the file name of the truststore file that contains authentication certificates for the HTTPS connection.
-TruststorePassword -tsp	truststore_password	Optional. Password for the truststore file.
-RulesServerPort -rpo	RulesServerPort	Optional. Port used by the rules server managed by the Interactive Data Preparation Service. Set the value to an available port on the node where the service runs.
-SolrPort -spo	SolrPort	Optional. Port number for the Apache Solr server used to provide data preparation recommendations.
-maxHeapSize -mxhs	maxHeapSize	Optional. Heap size to allocate to the service.
-FolderPath -fp	full_folder_path	Optional. Full path, excluding the domain name, to the folder in which you want to create the service. Must be in the following format:  <i>/parent_folder/child_folder</i>



# updateService

Updates Interactive Data Preparation Service properties.

The `infacmd idp updateService` command uses the following syntax:

```
updateService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-ServiceOptions|-so> option_name=value ...
(HDFSConnection*,HiveConnection*,HadoopConnection*,HDFSSystemDirectory*,HiveTableStorageF
ormat(DefaultFormat|Parquet|ORC (default DefaultFormat)),LogLevel(FATAL|ERROR|WARNING|
INFO|TRACE|DEBUG (default INFO)),customLogDirectory,SecurityMode(simple|kerberos
(default simple)),KerberosPrincipal(Principal Name for User
Impersonation),KerberosKeyTabFileName(SPN Keytab File for User Impersonation),
LogAuditEvents(true|false (default
false)),JDBCPort,ZeppelinURL,MaxFileUploadSize(default=512MB),DownloadRowsSize(default=10
00000),MaxRecommendations(default=10),MaxSampleSize(default=50000),SampleSize(default=500
00),hiveExecutionEngine(MR|Spark|Tez|Cluster-Default (default=Cluster-
Default),LocalSystemDirectory*,SolrJVMOptions,IndexDir)

<-RepositoryServiceName |-rs> repository_service_name

<-RepositoryUser|-rsun> repository_user

[<-RepositoryPassword|-rspd> repository_password]

[<-RepositorySecurityDomain|-rssdn> model_repository_security_domain]

<-DISServiceName|-dsn> dis_service_name

[<-NodeName|-nn> node_name]

[<-BackupNodes|-bn> node_name1,node_name2,...]

[<-ServiceProcessOptions|-po> option_name=value ...(HttpPort, HttpsPort, KeystoreFile,
KeystorePassword, TruststoreFile, TruststorePassword, RulesServerPort, SolrPort,
maxHeapSize ...)]
```

The following table describes infacmd idp updateService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.  If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-ServiceName -sn	service_name	<p>Required. Name of the Interactive Data Preparation Service.</p> <p>You cannot change the name of the service after you create it. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters:</p> <pre>` ~ % ^ * + = { } \ ; : ' " / ? . , &lt; &gt;   ! ( ) [ ]</pre>
-ServiceOptions -so	option_name=value ...	<p>Optional. Service properties that define how the service runs. To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks. You can define the following available service options:</p> <ul style="list-style-type: none"> <li>- HDFSCollection*</li> <li>- HiveConnection*</li> <li>- HadoopConnection*</li> <li>- HDFSSystemDirectory*</li> <li>- HiveTableStorageFormat(DefaultFormat Parquet ORC (default DefaultFormat))</li> <li>- LogLevel(FATAL ERROR WARNING INFO TRACE DEBUG (default INFO))</li> <li>- customLogDirectory</li> <li>- SecurityMode(simple kerberos (default simple))</li> <li>- KerberosPrincipal(Principal Name for User Impersonation)</li> <li>- KerberosKeyTabFileName(SPN Keytab File for User Impersonation)</li> <li>- LogAuditEvents(true false (default false))</li> <li>- JDBCPort</li> <li>- ZeppelinURL</li> <li>- MaxFileUploadSize(default=512MB)</li> <li>- DownloadRowsSize(default=1000000)</li> <li>- MaxRecommendations(default=10)</li> <li>- MaxSampleSize(default=50000)</li> <li>- SampleSize(default=50000)</li> <li>- hiveExecutionEngine(MR Spark Tez Cluster-Default (default=Cluster-Default))</li> <li>- LocalSystemDirectory*</li> <li>- SolrJVMOptions</li> <li>- IndexDir</li> </ul>
-RepositoryServiceName -rs	repository_service_name	<p>Optional. Name of the Model Repository Service that manages the Model repository that contains rule objects and metadata. Set this property if rules are used during data preparation.</p>
-RepositoryUser -rsun	-repository_username	<p>Optional. User account to use to log in to the Model Repository Service.</p>
-RepositoryPassword -rspd	-repository_password	<p>Optional. Password for the Model Repository Service user account.</p>

Option	Argument	Description
-RepositorySecurityDomain -rssdn	model_repository_security_domain	Optional. Security domain to which the Model Repository Service user account belongs.
-DISServiceName -dsn	dis_service_name	Optional. Name of the Data Integration Service that runs rules during data preparation. Set this property if rules are used during data preparation.
-NodeName -nn	node_name	Required if you do not specify grid name. Node where the service runs.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.
-ServiceProcessOptions -po	option_name=value ...	Optional. Service process properties for the service. In a multi-node environment, infacmd applies these properties to the primary node and backup node.

## upgradeRepository

Upgrades the contents of a Data Preparation repository.

The infacmd idp upgradeRepository command uses the following syntax:

```

upgradeRepository
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name

```

The following table describes infacmd idp upgradeRepository options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.  If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Interactive Data Preparation Service associated with the Data Preparation repository.

# KAPITEL 17

## infacmd edpl-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [createService, 315](#)
- [purgeauditevents, 320](#)
- [updateService, 322](#)
- [upgradeService, 326](#)

### createService

Creates an Enterprise Data Preparation Service.

The infacmd edp createService command uses the following syntax:

```
createService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

[<-Description|-des> description]

<-NodeName|-nn> node_name | <-GridName|-gn> grid_name

[<-BackupNodes|-bn> node_name1,node_name2,...]

<-ServiceOptions|-so> option_name=value ...
(HDFSConnection*,HiveConnection*,HadoopConnection*,HDFSSystemDirectory*,HiveTableStorageFormat(DefaultFormat|Parquet|ORC (default DefaultFormat)),LogLevel(FATAL|ERROR|WARNING|INFO|TRACE|DEBUG (default INFO)),customLogDirectory,SecurityMode(simple|kerberos (default simple)),KerberosPrincipal(Principal Name for User Impersonation),KerberosKeyTabFileName(SPN Keytab File for User Impersonation),LogAuditEvents(true|false (default false)),JDBCPort,ZeppelinURL,MaxFileUploadSize(default=512MB),DownloadRowsSize(default=100000),MaxRecommendations(default=10),MaxSampleSize(default=50000),SampleSize(default=5000),hiveExecutionEngine(MR|Spark|Tez|Cluster-Default (default=Cluster-Default)),LocalSystemDirectory*,SolrJVMOptions,IndexDir)

[<-LicenseName|-ln> license_name]
```

```

[<-HttpPort|-hp> http_port]
[<-HttpsPort|-hsp> https_port]
[<-KeystoreFile|-kf> keystore_file_location]
[<-KeystorePassword|-kp> keystore_password]
[<-TruststoreFile|-tf> truststore_file_location]
[<-TruststorePassword|-tp> truststore_password]
[<-FolderPath|-fp> full_folder_path]
<-RepositoryService|-rs> repository_service_name
<-RepositoryUser|-rsun> repository_user
[<-RepositoryPassword|-rspd> repository_password]
[<-RepositorySecurityDomain|-rssdn> model_repository_security_domain]
<-DataPreparationServiceName|-dpsn> data_preparation_service_name
<-DISServiceName|-dsn> dis_service_name
<-CatalogService|-ct> catalog_service_name
<-CatalogServiceUser|-ctun> catalogservice_user
<-CatalogServicePassword|-ctpd> catalogservice_password
[<-CatalogSecurityDomain|-cssdn> catalog_security_domain]

```

The following table describes infacmd edp createService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.



Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.  If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Enterprise Data Preparation Service.  You cannot change the name of the service after you create it. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < >   ! ( ) [ ]
-Description -des	description	Optional. Description of the service.
-NodeName -nn	node_name	Required if you do not specify grid name. Node where the service runs.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.

Option	Argument	Description
-ServiceOptions -so	option_name=value ...	Optional. Service properties that define how the service runs. To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks. You can define the following available service options: <ul style="list-style-type: none"> <li>- HDFSConnection*</li> <li>- HiveConnection*</li> <li>- HadoopConnection*</li> <li>- HDFSSystemDirectory*</li> <li>- HiveTableStorageFormat(DefaultFormat Parquet ORC (default DefaultFormat))</li> <li>- LogLevel(FATAL ERROR WARNING INFO TRACE DEBUG (default INFO))</li> <li>- customLogDirectory</li> <li>- SecurityMode(simple kerberos (default simple))</li> <li>- KerberosPrincipal(Principal Name for User Impersonation)</li> <li>- KerberosKeyTabFileName(SPN Keytab File for User Impersonation)</li> <li>- LogAuditEvents(true false (default false))</li> <li>- JDBCPort</li> <li>- ZeppelinURL</li> <li>- MaxFileUploadSize(default=512MB)</li> <li>- DownloadRowsSize(default=1000000)</li> <li>- MaxRecommendations(default=10)</li> <li>- MaxSampleSize(default=50000)</li> <li>- SampleSize(default=50000)</li> <li>- hiveExecutionEngine(MR Spark Tez Cluster-Default (default=Cluster-Default)</li> <li>- LocalSystemDirectory*</li> <li>- SolrJVMOptions</li> <li>- IndexDir</li> </ul>
-LicenseName -ln	license_name	Optional. License object that allows the use of the service.
-HttpPort -hp	http_port	Required if you do not specify an HTTPS port. Unique HTTP port number used for each Data Integration Service process. After you create the service, you can define different port numbers for each service process.
-HttpsPort -hsp	https_port	Required if you do not specify an HTTP port. Unique HTTPS port number used for each service process. After you create the service, you can define different port numbers for each service process.

Option	Argument	Description
-KeystoreFile -kf	keystore_file_location	Optional. Path and file name of the keystore file that contains the keys and certificates required if you use the HTTPS protocol for the service. You can create a keystore file with a keytool. keytool is a utility that generates and stores private or public key pairs and associated certificates in a keystore file. You can use the self-signed certificate or use a certificate signed by a certificate authority.
-KeystorePassword -kp	keystore_password	Optional. Password for the keystore file.
-TruststoreFile -tf	truststore_file_location	Optional. Path and the file name of the truststore file that contains authentication certificates for the HTTPS connection.
-TruststorePassword -tp	truststore_password	Optional. Password for the truststore file.
-FolderPath -fp	full_folder_path	Optional. Full path, excluding the domain name, to the folder in which you want to create the service. Must be in the following format:  <i>/parent_folder/child_folder</i>
-RepositoryService -rs	repository_service_name	Required. Name of the Model Repository Service to associate with the Enterprise Data Preparation Service.
-RepositoryUser -rsun	-repository_username	Required. User account to use to log in to the Model Repository Service.
-RepositoryPassword -rspd	-repository_password	Optional. Password for the Model Repository Service user account.
-RepositorySecurityDomain -rssdn	model_repository_security_domain	Optional. Security domain to which the Model Repository Service user account belongs.
-DataPreparationServiceName -dpsn	data_preparation_service_name	Required. Name of the Interactive Data Preparation Service to associate with the Enterprise Data Preparation Service.
-DISServiceName -dsn	dis_service_name	Required. Name of the Data Integration Service to associate with the Enterprise Data Preparation Service.
-CatalogService -ct	catalog_service_name	Required. Name of the Catalog Service to associate with the.

Option	Argument	Description
-CatalogServiceUser -ctun	catalogservice_user	Required. User account to use to log in to the Catalog Service.
-CatalogServicePassword -ctpd	catalogservice_password	Optional. Password for the Catalog Service user account.
-CatalogSecurityDomain -cssdn	catalog_security_domain	Optional. Security domain to which the Catalog Service user account belongs.

## purgeauditevents

Purges all Enterprise Data Preparation user activity events from the audit database. Optionally purges project history events from the audit database.

For more information about the events logged in the audit database, see the *Informatica Enterprise Data Preparation Administrator Guide*.

The `infacmd edp purgeauditevents` command uses the following syntax:

```

purgeauditevents
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-AuditDataRetentionPeriod|-rp> audit_data_retention_period_in_weeks
[<-PurgeProjectHistoryEvents|-phe> true|false]

```

The following table describes infacmd edp purgeauditevents options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.  If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-ServiceName -sn	service_name	Required. Name of the Enterprise Data Preparation Service for which to purge events.
-AuditDataRetentionPeriod -rp	audit_data_retention_period_in_weeks	Required. Number of weeks before the current calendar week for which to retain event data. The command does not purge data for the current calendar week. Specify 0 to retain data for one calendar week and purge prior log data. Specify 1 or greater to retain data for n + 1 calendar weeks and purge prior log data. For example, if you specify 1, the command retains data for two calendar weeks when it performs the purge. Minimum is 0.
PurgeProjectHistoryEvent -phe	true false	Optional. Purges project history events from the audit database. Set to true to purge project history from the audit database. Default is false.

## updateService

Updates an Enterprise Data Preparation Service.

The `infacmd edp updateService` command uses the following syntax:

```
updateService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-ServiceOptions|-so> option_name=value ...
(HDFSConnection*,HiveConnection*,HadoopConnection*,HDFSSystemDirectory*,HiveTableStorageFormat(DefaultFormat|Parquet|ORC (default DefaultFormat)),LogLevel(FATAL|ERROR|WARNING|INFO|TRACE|DEBUG (default INFO)),customLogDirectory,SecurityMode(simple|kerberos (default simple)),KerberosPrincipal(Principal Name for User Impersonation),KerberosKeyTabFileName(SPN Keytab File for User Impersonation),LogAuditEvents(true|false (default false)),JDBCPort,ZeppelinURL,MaxFileUploadSize(default=512MB),DownloadRowsSize(default=100000),MaxRecommendations(default=10),MaxSampleSize(default=50000),SampleSize(default=50000),hiveExecutionEngine(MR|Spark|Tez|Cluster-Default (default=Cluster-Default)),LocalSystemDirectory*,SolrJVMOptions,IndexDir)
<-NodeName|-nn> node_name | <-GridName|-gn> grid_name
```

```

[<-BackupNodes|-bn> node_name1,node_name2,...]

[<-ServiceProcessOptions|-po> option_name=value ...(httpPort, httpsPort, keystoreFile,
keystorePwd, truststoreFile, truststorePwd...)]

[<-RepositoryService|-rs> repository_service_name]

[<-RepositoryUser|-rsun> repository_user]

[<-RepositoryPassword|-rspd> repository_password]
[<-RepositorySecurityDomain|-rssdn> model_repository_security_domain]

[<-DataPreparationServiceName|-dpsn> data_preparation_service_name]

[<-DISServiceName|-dsn> dis_service_name]

[<-CatalogService|-ct> catalog_service_name]

[<-CatalogServiceUser|-ctun> catalogservice_user]

[<-CatalogServicePassword|-ctpd> catalogservice_password]

[<-CatalogSecurityDomain|-cssdn> catalog_security_domain]

```

The following table describes infacmd edp updateService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.</p> <p>If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.</p>
-ServiceName -sn	service_name	<p>Required. Name of the Enterprise Data Preparation Service.</p> <p>You cannot change the name of the service after you create it. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters:</p> <p>` ~ % ^ * + = { } \ ; : ' " / ? . , &lt; &gt;   ! ( ) [ ]</p>



Option	Argument	Description
-ServiceOptions -so	option_name=value ...	Optional. Service properties that define how the service runs. To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks. You can define the following available service options: <ul style="list-style-type: none"> <li>- HDFSConnection*</li> <li>- HiveConnection*</li> <li>- HadoopConnection*</li> <li>- HDFSSystemDirectory*</li> <li>- HiveTableStorageFormat(DefaultFormat Parquet ORC (default DefaultFormat))</li> <li>- LogLevel(FATAL ERROR WARNING INFO TRACE DEBUG (default INFO))</li> <li>- customLogDirectory</li> <li>- SecurityMode(simple kerberos (default simple))</li> <li>- KerberosPrincipal(Principal Name for User Impersonation)</li> <li>- KerberosKeyTabFileName(SPN Keytab File for User Impersonation)</li> <li>- LogAuditEvents(true false (default false))</li> <li>- JDBCPort</li> <li>- ZeppelinURL</li> <li>- MaxFileUploadSize(default=512MB)</li> <li>- DownloadRowsSize(default=1000000)</li> <li>- MaxRecommendations(default=10)</li> <li>- MaxSampleSize(default=50000)</li> <li>- SampleSize(default=50000)</li> <li>- hiveExecutionEngine(MR Spark Tez Cluster-Default (default=Cluster-Default))</li> <li>- LocalSystemDirectory*</li> <li>- SolrJVMOptions</li> <li>- IndexDir</li> </ul>
-NodeName -nn	node_name	Required if you do not specify grid name. Node where the service runs.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.
-ServiceProcessOptions -po	option_name=value ...	Optional. Service process properties for the service. In a multi-node environment, infacmd applies these properties to the primary node and backup node.
-RepositoryService -rs	repository_service_name	Optional. Name of the Model Repository Service to associate with the Enterprise Data Preparation Service.
-RepositoryUser -rsun	-repository_username	Optional. User account to use to log in to the Model Repository Service.
-RepositoryPassword -rspd	-repository_password	Optional. Password for the Model Repository Service user account.

Option	Argument	Description
- RepositorySecurityDomain -rssdn	model_repository_security_domain	Optional. Security domain to which the Model Repository Service user account belongs.
- DataPreparationServiceName -dpsn	data_preparation_service_name	Optional. Name of the Interactive Data Preparation Service to associate with the Enterprise Data Preparation Service.
-DISServiceName -dsn	dis_service_name	Optional. Name of the Data Integration Service to associate with the Enterprise Data Preparation Service.
-CatalogService -ct	catalog_service_name	Optional. Name of the Catalog Service to associate with the Enterprise Data Preparation Service.
-CatalogServiceUser -ctun	catalogservice_user	Optional. User account to use to log in to the Catalog Service.
- CatalogServicePassword -ctpd	catalogservice_password	Optional. Password for the Catalog Service user account.
- CatalogSecurityDomain -cssdn	catalog_security_domain	Optional. Security domain to which the Catalog Service user account belongs.

## upgradeService

Upgrades an Enterprise Data Preparation Service.

The infacmd edp upgradeService command uses the following syntax:

```

upgradeService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

```

The following table describes infacmd edp upgradeService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.  If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Enterprise Data Preparation Service to upgrade.

## KAPITEL 18

# Infacmd es-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [ListServiceOptions, 329](#)
- [UpdateServiceOptions, 330](#)
- [UpdateSMTPOptions, 331](#)

## ListServiceOptions

Gibt eine Liste mit Eigenschaften zurück, die für den E-Mail-Dienst konfiguriert sind. Zum Konfigurieren der Eigenschaften des E-Mail-Diensts führen Sie „infacmd es updateServiceOptions“ aus. Zum Konfigurieren der E-Mail-Server-Eigenschaften des E-Mail-Diensts führen Sie „infacmd es updateSMTPOptions“ aus.

Der infacmd es listServiceOptions-Befehl verwendet die folgende Syntax:

```
ListServiceOptions

<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
[<-ServiceName|-sn> service_name]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

**Hinweis:** Das infacmd-Programm stellt über die folgenden gemeinsamen Optionen eine Verbindung zur Domäne her: Domänenname, Benutzername, Passwort, Sicherheitsdomäne, Belastbarkeits-Timeout. Die Tabelle mit den Optionen enthält Kurzbeschreibungen. Detaillierte Beschreibungen finden Sie unter [„Herstellen einer Verbindung zur Domäne“ auf Seite 66](#).

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd es listServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.

Option	Argument	Beschreibung
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.
-ServiceName -sn	service_name	Optional. Geben Sie Email_Service ein.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.

## UpdateServiceOptions

Aktualisiert die Eigenschaften des E-Mail-Diensts. Führen Sie diesen Befehl zum Konfigurieren der Domäneneigenschaften und Knoten für den E-Mail-Dienst aus. Zum Anzeigen der aktuellen Eigenschaften des E-Mail-Diensts führen Sie „infacmd es listServiceOptions“ aus.

Der infacmd es updateServiceOptions-Befehl verwendet die folgende Syntax:

```
UpdateServiceOptions
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
[<-ServiceName|-sn> service_name]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-NodeName|nn> primary node name]
[<-BackupNodes|-bn> backup node names]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd es updateServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.

Option	Argument	Beschreibung
-Password -pd	password	Das Passwort für den Benutzernamen.
-ServiceName -sn	service_name	Optional. Geben Sie Email_Service ein.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-Options -o	options	Geben Sie die Optionen in folgendem Format ein: OptionGroupName.OptionName=OptionValue OptionGroupName2.OptionName2=OptionValue2  Führen Sie zum Anzeigen gültiger Optionen „infacmd isp ListServiceOptions“ aus.
-NodeName -nn	Name des primären Knotens	Optional. Primärer Knoten, auf dem der Dienst ausgeführt wird.
-BackupNodes -bn	Namen der Backup-Knoten	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist.

## UpdateSMTPOptions

Aktualisiert die SMTP-Eigenschaften für den E-Mail-Dienst. Geschäftsglossare und Arbeitsabläufe verwenden die SMTP-Konfiguration des E-Mail-Diensts zum Senden von Benachrichtigungen per E-Mail.

Die folgenden Benachrichtigungen verwenden die SMTP-Konfiguration des E-Mail-Diensts zum Senden von E-Mails:

- Business Glossary-Benachrichtigungen.
- Scorecard-Benachrichtigungen.
- Arbeitsablaufbenachrichtigungen. Zu den Arbeitsablaufbenachrichtigungen gehören E-Mails, die aus Human- und Benachrichtigungsaufgaben in Arbeitsabläufen gesendet werden, die der Datenintegrationsdienst ausführt.

Der infacmd es updateSMTPOptions-Befehl verwendet die folgende Syntax:

```
UpdateSMTPOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ServiceName|-sn> service_name]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
[<-SMTPServerHostName|-sa> smtp_host]
[<-SMTPUsername|-su> smtp_email_password]
[<-SMTPEmailPassword|-se> smtp_email_password]
[<-SMTPEmailAddress|-ss> smtp_email_address]
[<-SMTPPort|-sp> smtp_port]
[<-SMTPAuthEnabled|-sau> smtp_auth_enabled]
[<-SMTPTLSEnabled|-stls> smtp_tls_enabled]
[<-SMTPSSLEnabled|-sssl> smtp_ssl_enabled]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd es updateSMTPOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-ServiceName -sn	service_name	Optional. Geben Sie Email_Service ein.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-SMTPServerHostName -sa	smtp_host	Optional. Hostname für ausgehenden SMTP-Mailserver. Geben Sie zum Beispiel den Microsoft Exchange-Server für Microsoft Outlook ein. Standardwert ist „localhost“.
-SMTPUsername -su	smtp_user	Optional. Benutzername für die Authentifizierung beim Senden, wenn dies vom ausgehenden Mailserver gefordert wird.
-SMTPEmailPassword -se	smtp_email_password	Optional. Passwort für die Authentifizierung beim Senden, wenn dies vom ausgehenden SMTP-Mailserver gefordert wird.
-SMTPEmailAddress -ss	smtp_email_address	Optional. E-Mail-Adresse, die der E-Mail-Dienst beim Senden von Benachrichtigungs-E-Mails aus einem Arbeitsablauf im Feld „Von“ verwendet. Standardwert ist admin@example.com.



Option	Argument	Beschreibung
SMTPPort -sp	smtp_port	Optional. Portnummer, die vom ausgehenden SMTP-Mailserver verwendet wird. Die gültigen Werte liegen zwischen 1 und 65535. Standardwert ist 25.
-SMTPAuthEnabled -sau	smtp_auth_enabled	Optional. Gibt an, dass der SMTP-Server für die Authentifizierung aktiviert ist. Wenn TRUE, erfordert der ausgehende Mailserver einen Benutzernamen und ein Passwort. Wenn TRUE, müssen Sie angeben, ob der Server das TLS- (Transport Layer Security) oder das SSL-Protokoll (Secure Sockets Layer) verwenden soll. Geben Sie TRUE oder FALSE ein. Standardwert ist „false“.
-SMTPTLSEnabled -stls	smtp_tls_enabled	Optional. Gibt an, dass der SMTP-Server das TLS-Protokoll verwendet. Wenn TRUE, geben Sie die TLS-Portnummer für die Eigenschaft des SMTP-Serverports ein. Geben Sie TRUE oder FALSE ein. Standardwert ist „false“.
-SMTPSSLEnabled -sssl	smtp_ssl_enabled	Optional. Gibt an, dass der SMTP-Server das SSL-Protokoll verwendet. Wenn TRUE, geben Sie die SSL-Portnummer für die Eigenschaft des SMTP-Serverports an. Geben Sie TRUE oder FALSE ein. Standardwert ist „false“.

# KAPITEL 19

## infacmd ihs-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [cleanCluster, 334](#)
- [createservice, 336](#)
- [ListServiceOptions, 348](#)
- [ListServiceProcessOptions, 349](#)
- [shutdownCluster, 351](#)
- [UpdateServiceOptions, 353](#)
- [UpdateServiceProcessOptions, 354](#)

### cleanCluster

Bereinigt den Informatica-Cluster-Dienst. Wenn benutzerdefiniertes SSL für den Katalogdienst aktiviert ist, müssen Sie die folgenden Umgebungsvariablen festlegen:

- **INFA\_TRUSTSTORE.** Mithilfe des folgenden Beispielbefehls können Sie die Variable festlegen: `export INFA_TRUSTSTORE= <Speicherort der Informatica-Truststore-Datei>.`
- **INFA\_KEYSTORE.** Mithilfe des folgenden Beispielbefehls können Sie die Variable festlegen: `export INFA_KEYSTORE=<Speicherort der Schlüsselspeicherdatei>.`
- **Verschlüsseltes INFA\_TRUSTSTORE\_PASSWORD.** Verschlüsseln Sie das von Ihnen festgelegte Passwort. Mithilfe des folgenden Beispielbefehls können Sie das verschlüsselte Passwort festlegen: `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA==".`
- **Verschlüsseltes INFA\_KEYSTORE\_PASSWORD.** Verschlüsseln Sie das von Ihnen festgelegte Passwort. Mithilfe des folgenden Beispielbefehls können Sie das verschlüsselte Passwort festlegen: `export INFA_KEYSTORE_PASSWORD="6cDE/ItyUL/Rtui9nhVRI==".`

**Hinweis:** Mithilfe des folgenden Beispielbefehls können Sie das verschlüsselte Passwort festlegen: `$INFA_HOME/server/bin/pmpasswd <password>`

Beispiel:

- `export INFA_KEYSTORE_PASSWORD=hQDP8O8tfwxRSwbeANEptl4AIQqJcSj9ZMDkVK+9S+Y=`
- `export INFA_TRUSTSTORE_PASSWORD=hx/nRWisSjnQ0zEGV3N7j1FCGF0m5RfisQxKTdf5f8Y=`
- `export INFA_TRUSTSTORE=/data/Informatica/LDM1051/services/shared/security/`
- `export INFA_KEYSTORE=/data/Informatica/LDM1051/services/shared/security`

Der Befehl „infacmd ics cleanCluster“ verwendet folgende Syntax:

```
cleanCluster

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

**Hinweis:** Stellen Sie sicher, dass sich der Informatica-Cluster-Dienst im deaktivierten Zustand befindet, bevor Sie den Befehl ausführen.

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ics cleanCluster“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Informatica-Cluster-Diensts.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## createservice

Erstellt einen Informatica-Cluster-Dienst.

Der Befehl „infacmd ics createService“ verwendet die folgende Syntax:

```
CreateService
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-HttpPort|-p> port_name]
[<-HttpsPort|-sp> https_port_name]
[<-KeystoreFile|-kf> keystore_file_location]
[<-KeystorePassword|-kp> keystore_password]
[<-SSLProtocol|-ssl> ssl_protocol]
<-GatewayHost|-hgh> FQDN Host name of the node that serves as the gateway to the cluster
```

```

[<-DataNodes|-hn> Comma-separated list of fqdn host names that are data nodes of the
cluster. Mandatory if advance config is not enabled]

[<-ProcessingNodes|-pn> Comma-separated list of fqdn host names that are processing nodes
of the cluster

[<-GatewayUser|-gu> Username for the Gateway Node. Enable a Passwordless SSH connection
from Informatica Domain to Gateway Host for this user. Must be non-root sudo user

[<-ClusterCustomDir|-ccd> Cluster Custom Dir (default /opt/informatica/ics)]

[<-ClusterSharedFilesystemPath|-csfp> Cluster Shared Filesystem Path]

[<-OtherOptions|-oo> other options (specified in format:
[OptionGroupName.OptionName=OptionValue]. Multiple options can be separated by comma.
OptionValue should be specified within double quotes if it contains a comma.))

[<-BackupNodes|-bn> node_name1,node_name2,...]

[<-NomadServerHosts|-nsh> Nomad Server Hosts]

[<-NomadSerfPort|-nsp> Nomad Server Port (default 4648)]

[<-NomadHttpPort|-nhp> Nomad Http Port (default 4646)]

[<-NomadRpcPort|-nrp> Nomad RPC Port (default 4647)]

[<-NomadServerDir|-nsd> Nomad Server Dir (default $ClusterCustomDir/nomad/nomadserver)]

[<-NomadClientDir|-ncd> Nomad Client Dir (default $ClusterCustomDir/nomad/nomadclient)]

[<-NomadCustomOptions|-nco> Nomad Custom Options. (specified in format:
[OptionName=OptionValue]. Multiple options can be separated by comma. OptionValue should
be specified within double quotes if it contains a comma.))

[<-ZookeeperHosts|-zh> Zookeeper Hosts]

[<-ZookeeperPort|-zp> Zookeeper Port (default 2181)]

[<-ZookeeperPeerPort|-zpp> Zookeeper Peer Port (default 2888)]

[<-ZookeeperLeaderPort|-zlp> Zookeeper Leader Port (default 3888)]

[<-ZookeeperInstallDir|-zih> Zookeeper Install Dir (default $ClusterCustomDir/zk/
install)]

[<-ZookeeperDataDir|-zdd> Zookeeper Data Dir (default $ClusterCustomDir/zk/data)]

[<-ZookeeperCustomOptions|-zco> Zookeeper Custom Options. (specified in format:
[OptionName=OptionValue]. Multiple options can be separated by comma. OptionValue should
be specified within double quotes if it contains a comma.))

[<-SolrHosts|-sh> Solr Hosts]

[<-SolrPort|-sop> Solr Port (default 8983)]

[<-SolrInstallDir|-sih> Solr Install Dir (default $ClusterCustomDir/solr/install)]

[<-SolrDataDir|-sdd> Solr Data Dir (default $ClusterCustomDir/solr/data)]

[<-SolrCustomOptions|-sco> Solr Custom Options. (specified in format:
[OptionName=OptionValue]. Multiple options can be separated by comma. OptionValue should
be specified within double quotes if it contains a comma.))

[<-MongoHosts|-mdh> MongoDB Hosts]

[<-MongoPort|-mdp> MonogDB Port (default 27017)]

[<-MongoLogDir|-mdld> MongoDB Log Dir (default $ClusterCustomDir/mongo/log)]

```

```

[<-MongoDataDir|-mddd> MongoDB Data Dir (default $ClusterCustomDir/mongo/data)]

[<-MongoCustomOptions|-mco> MongoDB Custom Options. (specified in format:
[OptionName=OptionValue]. Multiple options can be separated by comma. OptionValue should
be specified within double quotes if it contains a comma.))

[<-PostgresHost|-pgh> Postgres Host]

[<-PostgresPort|-pgp> Postgres Port (default 5432)]

[<-PostgresInstallationDir|-pgdir> Postgres Install Dir (default $ClusterCustomDir/
postgres/install)]

[<-PostgresLogDir|-pgldir> Postgres Log Dir (default $ClusterCustomDir/postgres/log)]

[<-PostgresDataDir|-pgddir> Postgres Data Dir (default $ClusterCustomDir/postgres/data)]

[<-PostgresCustomOptions|-pgco> Postgres Custom Options. (specified in format:
[OptionName=OptionValue]. Multiple options can be separated by comma. OptionValue should
be specified within double quotes if it contains a comma.))

[<-ElasticHosts|-esh> elastic_hosts]

[<-ElasticHttpPort|-eshp> elastic_httpport]

[<-ElasticTcpPort|-estp> elastic_tcpport]

[<-ElasticLogDir|-esld> elastic_log_dir]

[<-ElasticDataDir|-esdd> elastic_data_dir]

[<-ElasticClusterName|-escn> elastic_cluster_name]

[<-ElasticEnableTls|-etls> elastic_enable_tls true|false (default false)]

[<-ElasticUserName|-eun> elastic_user_name]

[<-ElasticPassword|-epswd> elastic_password]

[<-SparkMasterNode|-smn> spark_master_node]

[<-SparkMasterPort|-smp> spark_master_port]

[<-SparkSlaveNodes|-ssn> spark_slave_nodes]

[<-SparkExecutorCores|-sec> spark_executor_cores]

[<-SparkLogDir|-sld> spark_logdir]

[<-DPMEEnable|-dpme> Enable DPM true|false (default false)]

[<-DPMEEnableAdvanceConfig|-dpmeadv< Enable DPM Advance Config true|false (default
false)]

[<-EnableAdvanceConfig|-eadvc> Enable Advance Config true|false (default false)]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ics CreateService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-NodeName -nn	node_name	Erforderlich. Knotenname der Informatica-Domäne.
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-ServiceName -sn	service_name	Erforderlich. Name des Informatica-Cluster-Diensts.
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-HttpPort -p	port_name	<p>Optional. Eine eindeutige HTTP-Portnummer, die für den Informatica-Cluster-Dienst verwendet wird. Die Standardportnummer lautet 9075.</p>



Option	Argument	Beschreibung
-HttpsPort -sp	https_port_name	Erforderlich, wenn Sie „Transport Layer Security“ aktivieren. Die Portnummer für die HTTPS-Verbindung.
-KeystoreFile -kf	keystore_file_location	Erforderlich, wenn Sie „Transport Layer Security aktivieren“ auswählen. Pfad und Dateiname der Schlüsselspeicherdatei. Die Schlüsselspeicherdatei enthält die Schlüssel und Zertifikate, die bei Verwendung des SSL-Sicherheitsprotokolls mit Catalog® Administrator erforderlich sind.
-KeystorePassword -kp	keystore_password	Erforderlich, wenn Sie „Transport Layer Security aktivieren“ auswählen. Das Passwort für die Schlüsselspeicherdatei.
-SSLProtocol -sslp	ssl_protocol	Optional. Secure Sockets Layer-Protokoll (SSL), das verwendet werden soll.
-GatewayHost -hgh	gateway_host	Erforderlich. Hostname des vollqualifizierten Domännennamens (FQDN) des Knotens, der als Gateway zum Informatica-Cluster dient.
-DataNodes -hn	data_nodes	Eine durch Kommas getrennte Liste von FQDN-Hostnamen, die Datenknoten des Informatica-Clusters sind. Obligatorisch, wenn die erweiterte Konfiguration nicht aktiviert ist.
-ProcessingNodes -pn	processing_nodes	Eine durch Kommas getrennte Liste von FQDN-Hostnamen, die Knoten des Informatica-Clusters verarbeiten.
-GatewayUser -gu	gateway_user	Der Benutzername für den Gateway-Knoten. Aktivieren Sie eine SSH-Verbindung ohne Passwort von der Informatica-Domäne zum Gateway-Host für den aktuellen Benutzer. Der Benutzer muss ein Nicht-Root-Sudo-Benutzer sein.
-ClusterCustomDir -ccd	cluster_custom_dir	Das benutzerdefinierte Clusterverzeichnis. Beispiel: default /opt/ informatica/ics

Option	Argument	Beschreibung
-ClusterSharedFilesystemPath -csfp	cluster_shared_filesystem_path	Erforderlich, wenn der Informatica-Cluster-Dienst für mehrere Knoten eingerichtet ist. Der Pfad des gemeinsam genutzten Cluster-Dateisystems.
-OtherOptions -oo	other_options	Mehrere Optionen, die durch ein Komma getrennt werden können. Der Optionswert sollte in doppelten Anführungszeichen angegeben werden, wenn er ein Komma enthält. Das angegebene Format lautet: [OptionGroupName.OptionName=OptionValue].
-BackupNodes -bn	node_name1,node_name2,...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Backup-Knoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.
-NomadServerHosts -nsh	nomad_server_hosts	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie die durch Kommas getrennten Nomad-Serverhosts an.
-NomadSerfPort -nsp	nomad_service_port	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie den Nomad-Serverport an. Der Standardwert ist 4648.
-NomadHttpPort -nhp	nomad_http_port	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie den Nomad-HTTP-Port an. Der Standardwert ist 4646.
-NomadRpcPort -nrp	nomad_rpc_port	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie den Nomad-RPC-Port an. Der Standardwert ist 4647.
-NomadServerDir -nsd	nomad_server_dir	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie das Nomad-Serververzeichnis an. Beispiel: default \$ClusterCustomDir/ nomad/nomadserver

Option	Argument	Beschreibung
-NomadClientDir -ncd	nomad_client_dir	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie das Nomad-Clientverzeichnis an. Beispiel: default \$ClusterCustomDir/nomad/nomadclient
-NomadCustomOptions -nco	nomad_custom_options	Optional. Geben Sie den durch Kommas getrennten Optionswert in doppelten Anführungszeichen an, wenn der Wert ein Komma enthält. Angegebenes Format: [OptionName=OptionValue]
-ZookeeperHosts -zh	zookeeper_hosts	Geben Sie die Zookeeper-Hosts mit durch Kommas getrennten Werten an.
-ZookeeperPort -zp	zookeeper_port	Geben Sie den Zookeeper-Port an. Der Standardwert ist 2181.
-ZookeeperPeerPort -zpp	zookeeper_peer_port	Geben Sie den Zookeeper-Peer-Port an. Der Standardwert ist 2888.
-ZookeeperLeaderPort -zlp	zookeeper_leader_port	Geben Sie den Zookeeper-Leader-Port an. Der Standardwert ist 3888.
-ZookeeperInstallDir -zih	zookeeper_install_dir	Geben Sie das Zookeeper-Installationsverzeichnis an: (default \$ClusterCustomDir/zk/install)]
-ZookeeperDataDir -zdd	zookeeper_data_dir	Geben Sie das Zookeeper-Datenverzeichnis an: (default \$ClusterCustomDir/zk/data)]
-ZookeeperCustomOptions -zco	zookeeper_custom_options	Optional. Die durch Kommas getrennten benutzerdefinierten Zookeeper-Optionen. Geben Sie die Option im folgenden Format an: [OptionName=OptionValue] Geben Sie die Optionswerte in doppelten Anführungszeichen an, wenn die Werte ein Komma enthalten.
-SolrHosts -sh	solr_hosts	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie die Solr-Hosts an.

Option	Argument	Beschreibung
-SolrPort -sop	solr_port	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie den Solr-Port an. Der Standardwert ist 8983.
-SolrInstallDir -sih	solr_install_dir	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie das Solr-Installationsverzeichnis an. Der Standardwert ist \$ClusterCustomDir/solr/install.
-SolrDataDir -sdd	solr_data_dir	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie das Solr-Datenverzeichnis an. Der Standardwert ist \$ClusterCustomDir/solr/data
-SolrCustomOptions -sco	solr_custom_options	Optional. Geben Sie die benutzerdefinierten Solr-Optionen an. Geben Sie die Optionen im folgenden Format an: [OptionName=OptionValue]. Mehrere Optionen können durch Kommas getrennt werden. Geben Sie den Optionswert in doppelten Anführungszeichen an, wenn der Wert ein Komma enthält.
-MongoHosts -mdh	mongo_db_hosts	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie die MongoDB-Hosts an.
-MongoPort -mdp	mongo_port	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie den MongoDB-Port an. Die Standardportnummer lautet 27017.
-MongoLogDir -mdld	mongo_log_dir	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie das MongoDB-Protokollverzeichnis an. Der Standardwert ist \$ClusterCustomDir/mongo/log

Option	Argument	Beschreibung
-MongoDataDir -mddd	mongo_data_dir	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie das MongoDB-Datenverzeichnis an. Das Standardverzeichnis ist <code>\$ClusterCustomDir/mongo/data</code>
-MongoCustomOptions -mco	mongo_custom_options	Optional. Geben Sie die benutzerdefinierten MongoDB-Optionen an. Geben Sie die benutzerdefinierten Optionen im folgenden Format an: [OptionName=OptionValue]. Trennen Sie mehrere Optionen durch ein Komma. Geben Sie den Optionswert in doppelten Anführungszeichen an, wenn die Werte ein Komma enthalten.
-PostgresHost -pgh	postgres_host	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie den Postgres-Host an.
-PostgresPort -pgp	postgres_port	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie den Postgres-Port an. Die Standardportnummer lautet 5432.
-PostgresInstallationDir -pgdir	postgres_installation_dir	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie das Postgres-Installationsverzeichnis an. Das Standardverzeichnis ist <code>\$ClusterCustomDir/postgres/install</code>
-PostgresLogDir -pgldir	postgres_log_dir	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie das Postgres-Protokollverzeichnis an. Das Standardverzeichnis ist <code>\$ClusterCustomDir/postgres/log</code> .

Option	Argument	Beschreibung
-PostgresDataDir -pgddir	postgres_data_dir	Erforderlich Wenn Sie die erweiterte Konfigurationseigenschaft aktivieren, wird „-eadvc“ auf „true“ gesetzt. Geben Sie das Postgres-Datenverzeichnis an. Das Standardverzeichnis ist <code>\$ClusterCustomDir/postgres/data</code> .
-PostgresCustomOptions -pgco	postgres_custom_options	Optional. Geben Sie die benutzerdefinierten Postgres-Optionen an. Geben Sie die benutzerdefinierten Optionen im folgenden Format an: [OptionName=OptionValue]. Mehrere Optionen können durch Kommas getrennt werden. Geben Sie den Optionswert in doppelten Anführungszeichen an, wenn der Wert ein Komma enthält.
-ElasticHosts -esh	elastic_hosts	Geben Sie den Elastic-Hostnamen des Computers an, auf dem Elasticsearch installiert ist. Sie können mehrere Hostnamen durch Kommas getrennt eingeben.
-ElasticHttpPort -eshp	elastic_httpport	Geben Sie die Portnummer für Elasticsearch an, die Data Privacy Management verwendet, um eine Verbindung zur Web-Benutzeroberfläche von Elasticsearch herzustellen. Der Standardwert ist 9200.
-ElasticTcpPort -estp	elastic_tcpport	Geben Sie die Portnummer für Elasticsearch an, die Data Privacy Management verwendet, um eine Verbindung zur Elasticsearch-Anwendung herzustellen. Der Standardwert ist 9300.
-ElasticLogDir -esld	elastic_log_dir	Geben Sie das Elastic-Protokollverzeichnis an. Der Speicherort für die Elasticsearch-Protokolldateien. Der Standardwert ist <code>/var/log/elasticsearch</code> .
-ElasticDataDir -esdd	elastic_data_dir	Geben Sie das Elastic-Datenverzeichnis an. Der Speicherort für Data Privacy Management-Daten in Elasticsearch. Standardwert ist <code>/var/lib/elasticsearch</code> .
-ElasticClusterName -escn	elastic_cluster_name	Geben Sie den Namen des Elasticsearch-Clusters an.

Option	Argument	Beschreibung
-ElasticEnableTls -etls	elastic_enable_tls	Wählen Sie die Option zum Aktivieren von TLS (Transport Layer Security) für den Dienst aus. Der Standardwert ist FALSE.
-ElasticUserName -eun	elastic_user_name	Geben Sie den SSL-Benutzernamen für Elasticsearch an.
-ElasticPassword -epswd	elastic_password	Geben Sie das SSL-Passwort für Elasticsearch an.
-SparkMasterNode -smn	spark_master_node	Geben Sie den Namen des Spark-Masterknotens an. Dies muss der Gateway-Knoten des Informatica-Cluster-Diensts sein.
-SparkMasterPort -smp	spark_master_port	Geben Sie die Portnummer an, die Data Privacy Management für die Verbindung zum Spark-Masterknoten verwendet.
-SparkSlaveNodes -ssn	spark_slave_nodes	Geben Sie die Spark-Slave-Knoten an. Slave-Knoten befinden sich in der Regel auf Verarbeitungsknoten. Mehrere Werte können durch Kommas getrennt werden.
-SparkExecutorCores -sec	spark_executor_cores	Anzahl der verwendeten Spark-Executor-Kerne.
-SparkLogDir -sld	spark_log_dir	Geben Sie das Spark-Protokollverzeichnis an. Der Speicherort für die Spark-Protokolldateien. Der Standardwert ist <code>/var/log/spark</code> .
-DPMEnable -dpme	dpm_enable	Aktivieren Sie die Benutzeraktivität, die Informatica-Cluster-Dienste verwendet. Der Standardwert ist FALSE.
-DPMEnableAdvanceConfig -dpmeadv	dpm_enable_advance_config	Konfigurieren Sie die Eigenschaften der Anwendungen und zugehörigen Dienste von DPM. Der Standardwert ist FALSE.
-EnableAdvanceConfig -eadvc	enable_advance_config	Konfigurieren Sie die Eigenschaften der Anwendungen und zugehörigen Dienste. Der Standardwert ist FALSE.

# ListServiceOptions

Listet Optionen für den Informatica-Cluster-Dienst auf.

Der Befehl „infacmd ics ListServiceOptions“ verwendet die folgende Syntax:

```
ListServiceOptions  
  
<-DomainName|-dn> domain_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
<-ServiceName|-sn> service_name  
  
[<-SecurityDomain|-sdn> security_domain]  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ics ListServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Informatica-Cluster-Diensts.



Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## ListServiceProcessOptions

Listet die Prozessoptionen für den Informatica-Cluster-Dienst auf.

Der Befehl „infacmd ics ListServiceProcessOptions“ verwendet die folgende Syntax:

```
ListServiceProcessOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ics ListServiceProcessOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Informatica-Cluster-Diensts.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienstprozess ausgeführt wird.

## shutdownCluster

Führt den Informatica-Cluster-Dienst und die entsprechenden Dienste wie Nomad, Solr, MongoDB und Postgres SQL herunter. Wenn benutzerdefiniertes SSL für den Katalogdienst aktiviert ist, müssen Sie die folgenden Umgebungsvariablen festlegen:

- **INFA\_TRUSTSTORE.** Mithilfe des folgenden Beispielbefehls können Sie die Variable festlegen: `export INFA_TRUSTSTORE= <Speicherort der Informatica-Truststore-Datei>.`
- **INFA\_KEYSTORE.** Mithilfe des folgenden Beispielbefehls können Sie die Variable festlegen: `export INFA_KEYSTORE=<Speicherort der Schlüsselspeicherdatei>.`
- **Verschlüsseltes INFA\_TRUSTSTORE\_PASSWORD.** Verschlüsseln Sie das von Ihnen festgelegte Passwort. Mithilfe des folgenden Beispielbefehls können Sie das verschlüsselte Passwort festlegen: `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA==".`
- **Verschlüsseltes INFA\_KEYSTORE\_PASSWORD.** Verschlüsseln Sie das von Ihnen festgelegte Passwort. Mithilfe des folgenden Beispielbefehls können Sie das verschlüsselte Passwort festlegen: `export INFA_KEYSTORE_PASSWORD="6cDE/ItyUL/Rtui9nhVRI==".`

**Hinweis:** Mithilfe des folgenden Beispielbefehls können Sie das verschlüsselte Passwort festlegen: `$INFA_HOME/server/bin/pmpasswd <password>`

Beispiel:

- `export INFA_KEYSTORE_PASSWORD=hQDP8O8tfwxRSwbeANEptl4AIQqJcSj9ZMDkVK+9S+Y=`
- `export INFA_TRUSTSTORE_PASSWORD=hx/nRWisSjnQ0zEGV3N7j1FCGF0m5RfisQxKTdf5f8Y=`
- `export INFA_TRUSTSTORE=/data/Informatica/LDM1051/services/shared/security/`
- `export INFA_KEYSTORE=/data/Informatica/LDM1051/services/shared/security`

Der Befehl „infacmd.sh ics shutdownCluster“ verwendet die folgende Syntax:

```
shutdownCluster

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-SecurityDomain|-sdn> security_domain]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd.sh ics shutdownCluster“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Bezieht sich auf den Namen des Informatica-Cluster-Diensts.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

# UpdateServiceOptions

Aktualisiert die Serviceoptionen des Informatica-Cluster-Diensts. Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Der Befehl „infacmd ics UpdateServiceOptions“ verwendet die folgende Syntax:

```
UpdateServiceOptions  
  
<-DomainName|-dn> domain_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
<-ServiceName|-sn> service_name  
  
[<-SecurityDomain|-sdn> security_domain]  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]  
  
<-Options|-o> options  
  
[<-PrimaryNode|-nn> node_name]  
  
[<-BackupNodes|-bn> node_name1,node_name2,...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ics UpdateServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Informatica-Cluster-Diensts.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Options -o	options	Erforderlich. Geben Sie Name-Wert-Paare durch Leerzeichen getrennt ein.  Wenn Sie Service Pack 10.5.1.1 oder eine spätere Version angewendet haben, können Sie das SSL-Protokoll für den Informatica-Cluster-Dienst mithilfe der Option <code>GeneralOptions.SSLProtocol</code> auf TLS 1.1 oder TLS 1.2 konfigurieren. Geben Sie einen der folgenden Werte an: - TLSv1.1 - TLSv1.2
-PrimaryNode -nn	node_name	Optional. Primärer Knoten, auf dem der Informatica-Cluster-Dienst ausgeführt wird.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Knoten, auf denen der Informatica-Cluster-Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Backup-Knoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.

## UpdateServiceProcessOptions

Aktualisiert die Dienstprozessoptionen des Informatica-Cluster-Diensts. Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Der Befehl „infacmd ics UpdateServiceProcessOptions“ verwendet die folgende Syntax:

```
UpdateServiceProcessOptions
<-DomainName|-dn> domain_name
```

```

<-nodeName|-nn> node_name

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Options|-o> options

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ics UpdateServiceProcessOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienstprozess ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Informatica-Cluster-Diensts.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-Options -o	options	<p>Erforderlich. Geben Sie Name-Wert-Paare durch Leerzeichen getrennt ein.</p>



## KAPITEL 20

# infacmd ipc-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [ExportToPC, 357](#)
- [ImportFromPC, 361](#)
- [genReuseReportFromPC, 363](#)

## ExportToPC

Exportiert Objekte aus dem Modellrepository oder einer Exportdatei und konvertiert sie in PowerCenter-Objekte.

Mit dem Befehl ExportToPC werden Objekte aus dem Modellrepository oder aus einer aus dem Modellrepository exportierten XML-Datei konvertiert. Sie müssen entweder ein Modellrepository oder eine Quelldatei für den Export auswählen. Wenn Sie beide Optionen auswählen, hat die Quelldateioption Vorrang. Führen Sie den Befehl ExportToPC aus, um eine XML-Datei zu erstellen, die Sie mit dem pmrep-Programm in PowerCenter importieren können.

Der Befehl „infacmd ipc ExportToPC“ verwendet die folgende Syntax:

```
ExportToPC
<-Release|-rel> release_number
[<-SourceFile|-sf> source_file]
[<-SourceRepository|-sr> source_repository]
[<-SourceFolders|-f> folder1 folder2|<-SourceObjects|-so> source_objects]
[<-Recursive|-r>]
[<-TargetLocation|-tl> target_location]
[<-TargetFolder|-tf> target_folder_name]
[<-CodePage|-cp> target_code_page]
[<-Check|-c>]
[<-ReferenceDataLocation|-rdl> reference_data_output_location]
[<-ConvertMappletTargets|-cmt>]
[<-ConvertMappingsToMapplets|-cmm>]
[<-NoValidation|-nv>]
```

[<-DSTErrorFormat|-def>]

[<-OptimizationLevel|- 0 optimization\_level 1 or Optimization\_level 2]

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ipc ExportToPC“ beschrieben:

Option	Argument	Beschreibung
-Release -rel	release_number	Erforderlich. Die PowerCenter Versionsnummer.
-SourceFile -sf	source_file	Optional. Den vollständigen Pfad zu einer XML-Datei, die mit dem Developer Tool exportierte Quellobjekte enthält.

Option	Argument	Beschreibung
-SourceRepository -sr	source_repository	<p>Optional. Das Modellrepository, das die nach PowerCenter zu exportierenden Objekte enthält.</p> <p>Verwenden Sie die folgende Befehlssyntax in einer Domäne ohne Kerberos-Authentifizierung, um den Gateway-Host und den Port für die Verbindung zum Modellrepository-Dienst anzugeben:</p> <pre>&lt;Model repository name&gt;@&lt;host&gt;:&lt;port&gt;#&lt;projectname&gt; ? user=&lt;username&gt;[&amp;namespace=&lt;namespace&gt;]&amp;password=&lt;password&gt;</pre> <p>Verwenden Sie zum Angeben des Domänennamens, wenn Sie mehrere Gateway-Knoten haben, die folgende Befehlssyntax, um eine stabile Verbindung zum Modellrepository-Dienst in einer Domäne ohne Kerberos-Authentifizierung herzustellen:</p> <pre>&lt;Model repository name&gt;@&lt;domainname&gt;#&lt;projectname&gt; ? user=&lt;username&gt;[&amp;namespace=&lt;namespace&gt;]&amp;password=&lt;password&gt;</pre> <p>Verwenden Sie die folgende Befehlssyntax zum Angeben des Domänennamens mit den eingegebenen Anmeldedaten, um den Befehl mit Single Sign-On auszuführen:</p> <pre>&lt;Model repository name&gt;@&lt;domainname&gt;#&lt;projectname&gt; ?isloggedinuser=true[&amp;namespace=&lt;namespace&gt;]</pre> <p>Verwenden Sie die folgende Befehlssyntax zum Angeben des Gateway-Hosts und des Ports mit den eingegebenen Anmeldedaten, um den Befehl mit Single Sign-On auszuführen:</p> <pre>&lt;Model repository name&gt;@&lt;host&gt;:&lt;port&gt;#&lt;projectname&gt; ?isloggedinuser=true[&amp;namespace=&lt;namespace&gt;]</pre> <p>Verwenden Sie die folgende Befehlssyntax in einer Kerberos-Domäne zum Angeben des Gateway-Hosts und des Ports mit den Anmeldedaten, die Sie statt der eingegebenen Anmeldedaten angeben:</p> <pre>&lt;Model repository name&gt;@&lt;host&gt;:&lt;port&gt;#&lt;projectname&gt; ? iskerberos=true&amp;user=&lt;username&gt;[&amp;namespace=&lt;namespace&gt;]&amp;password=&lt;password&gt; &amp;Kerberosrealm=&lt;kerberosrealm&gt;</pre> <p>Verwenden Sie die folgende Befehlssyntax in einer Kerberos-Domäne zum Angeben des Domänennamens mit den Anmeldedaten, die Sie statt der eingegebenen Anmeldedaten angeben:</p> <pre>&lt;Model repository name&gt;@&lt;domainname&gt;#&lt;projectname&gt; ? iskerberos=true&amp;user=&lt;username&gt;[&amp;namespace=&lt;namespace&gt;]&amp;password=&lt;password&gt; &amp;Kerberosrealm=&lt;kerberosrealm&gt;</pre> <p>Der Portparameter ist der HTTP-Port. Der &amp;namespace-Parameter ist optional. Der Standardnamespace ist nativ.</p>
-SourceFolders -f	source_folders	<p>Wenn Sie -sr verwenden, müssen Sie -f oder -so verwenden.</p> <p>Liste der Quellordner, die aus dem Modellrepository exportiert werden sollen. Sie können Mapplets, Mappings und logische Datenobjektmodelle aus den Quellordnern nach PowerCenter exportieren. Wenn Sie mehr als ein Objekt exportieren, müssen Sie die Objekte in der Liste durch ein Leerzeichen voneinander trennen.</p>

Option	Argument	Beschreibung
SourceObjects -so	source_objects	<p>Wenn Sie -sr verwenden, müssen Sie -f oder -so verwenden.</p> <p>Liste der Quellobjekte, die aus dem Modellrepository exportiert werden sollen. Sie können Mapplets, Mappings und logische Datenobjektmodelle nach PowerCenter exportieren. Sie können das Objekt als Name beschreiben. Verwenden Sie folgende Syntax:</p> <pre>name=/&lt;path&gt;/&lt;objectname&gt; [&amp;type=&lt;typename&gt;]</pre> <p>Sie müssen den vollständigen Pfad des Objekts angeben. Wenn Sie mehr als ein Objekt exportieren, müssen Sie die Objekte in der Liste durch ein Leerzeichen voneinander trennen.</p> <p>Sie können die folgenden Typen eingeben:</p> <ul style="list-style-type: none"> <li>- Mapping. Verwenden Sie diesen Typ zum Exportieren von Mappings und Mapplets.</li> <li>- DataObjectModel. Verwenden Sie diesen Typ zum Exportieren logischer Datenobjektmodelle.</li> </ul> <p>Bei diesem Typ wird nicht zwischen Groß- und Kleinschreibung unterschieden. Standardwert ist „Mapping“.</p>
-Recursive -r	-	<p>Optional. Exportiert alle Mappings und logischen Datenobjektmodelle aus den Quellordnern. Exportiert jeden Unterordner unterhalb der Objekte und alle Unterordner darunter.</p> <p>Der Standardwert ist „false“.</p>
-TargetLocation -tl	target_location	Optional. Der vollständige Pfad zur XML-Target-Datei.
-TargetFolder -tf	target_folder_name	Optional. Der PowerCenter-Ordner, in den die Objekte exportiert werden. Der Befehl ExportToPC platziert den Ordernamen in der XML-Target-Datei. Wenn Sie keinen Ordernamen konfigurieren, erstellt der Befehl ExportToPC einen Ordernamen.
-CodePage -cp	target_code_page	Optional. Codepage des PowerCenter-Repository. Standardwert ist UTF-8.
-Check -c	-	<p>Optional. Testet die Umwandlung, ohne eine Zielfeile zu erstellen.</p> <p>Der Standardwert ist „false“.</p>
-ReferenceDataLocation -rdl	reference_data_output_location	Optional. Speicherort, an dem Sie Referenztabellendaten ablegen möchten. Der Befehl „ExportToPC“ speichert die Referenztabellendaten als eine oder mehrere Wörterbuch-Dateien (.dic).
-ConvertMappletTargets -cmt	-	<p>Optional. Wandelt Ziele in Mapplets in Ausgabeumwandlungen im PowerCenter-Mapplet um.</p> <p>PowerCenter-Mapplets dürfen keine Ziele enthalten. Wenn der Export ein Mapplet einschließt, das ein Ziel enthält und Sie diese Option nicht auswählen, schlägt der Exportprozess fehl.</p> <p>Der Standardwert ist „false“.</p>
-ConvertMappingstoMapplets -cmm	-	<p>Optional. Wandelt Developer-Tool-Mappings in PowerCenter-Mapplets um. Das Developer-Tool wandelt Quellen und Ziele in den Mappings in Eingabe- und Ausgabeumwandlungen in einem PowerCenter-Mapplet um.</p> <p>Der Standardwert ist „false“.</p>

Option	Argument	Beschreibung
-NoValidation -nv	-	Optional. Quellobjekte werden vor ihrer Umwandlung nicht über den Befehl ExportToPC validiert. Der Standardwert ist „false“.
-DSErrorFormat -def	-	Optional. Die Fehlermeldungen werden in einem Format angezeigt, das vom Developer Tool analysiert werden kann. Der vollständige Pfad jedes Objekts wird in den Fehlermeldungen angezeigt. Standardmäßig werden Fehler in einem benutzerfreundlichen Format angezeigt.
OptimizationLevel . - 0	optimization_level	Optional. Steuert die Optimierungsmethoden, die der Datenintegrationsdienst auf die Zuordnung anwendet. Geben Sie den numerischen Wert ein, der mit der Optimierungsebene verbunden ist, die Sie konfigurieren möchten. Geben Sie einen der folgenden numerischen Werte ein: <ul style="list-style-type: none"> <li>- 0 (Keine). Der Datenintegrationsdienst wendet keine Optimierung an.</li> <li>- 1 (Minimal). Der Datenintegrationsdienst wendet die Optimierungsmethode der frühen Projektion an.</li> <li>- 2 (Normal). Der Datenintegrationsdienst wendet folgende Optimierungsmethoden an: frühe Projektion, frühe Auswahl, Verzweigungsereinigung, Push-Into, Pushdown und Prädikat. Normal ist die Standardoptimierungsebene.</li> <li>- 3 (Vollständig). Der Datenintegrationsdienst wendet folgende Optimierungsmethoden an: kostenbasiert, frühe Projektion, frühe Auswahl, Verzweigungsereinigung, Prädikat, Push-Into, Pushdown und Semi-Join.</li> </ul> Wenn Sie diese Option nicht verwenden, wendet der Datenintegrationsdienst die Optimierungsebene an, die in den Zuordnungseigenschaften für die bereitgestellte Anwendung im Administrator Tool konfiguriert wurde.

## ImportFromPC

Wandelt eine XML-Datei eines PowerCenter-Repository-Objekts in eine XML-Datei eines Modellrepository-Objekts um. PowerCenter-Repository-Objekte in eine XML-Datei exportieren. Führen Sie den Befehl „importFromPC“ aus, um eine XML-Zieldatei mit Objekten zu erstellen, die in ein Modellrepository importiert werden können.

Sie können die XML-Zieldatei mit dem Befehl „infacmd tools ImportObjects“ oder über das Developer Tool in ein Modellrepository importieren. Wenn Sie die Befehlszeile zum Importieren der Ziel-XML-Datei verwenden, weist ImportFromPC den Modellrepository-Objekten in der Ziel-XML-Datei keine Verbindungen zu. Sie können Verbindungen mit dem infacmd oie ImportObjects-Befehl oder über das Developer Tool zuweisen.

Der infacmd ipc importFromPC-Befehl verwendet die folgende Syntax:

```
importFromPC
<-Release|-rel> release_number
[<-SourceFile|-sf> source_file]
[<-TargetFile|-tf> target_location]
[<-Check|-c>]
[<-Db2Type|-dt> default_db2_type]
```

```
[<-Db2TypesFile|-df> db2_types_file]

[<-DefaultLookUpConType|-dl> default_lookup_con_type]

[<-LookUpConTypesFile|-lcf> lookup_connection_types_file]

[<-ConvertOverriddenProps|-orprops> recreate_transformation_with_overridden_properties_in_mappings]

[<-LogFile|-lf> log_file]
```

In der folgenden Tabelle werden die Optionen und Argumente des infacmd ipc ImportFromPC-Befehls beschrieben:

Option	Argument	Beschreibung
-Release -rel	release_number	Erforderlich. Die Version des Modellrepositors.
-SourceFile -sf	source_file	Erforderlich. Der vollständige Pfad einer PowerCenter-XML-Datei, die die Quellobjekte enthält.
-TargetFile -tf	target_location	Erforderlich, wenn Sie nicht -Check oder -c angeben. Der vollständige Pfad zu einer XML-Zielfeile.
-Check -c	-	Optional. Testet die Umwandlung, ohne eine Zielfeile zu erstellen. Wenn Sie die Objektumwandlung testen, benötigen Sie keinen Zielspeicherort.
-Db2Type -dt	default_db2_type	Optional. Der für die Umwandlung verwendete DB2-Subsystemtyp. Sie können entweder Db2Type oder DB2TypesFile oder beides angeben. Wenn Sie sowohl Db2Type als auch Db2TypesFile für IBM DB2-Objekte angeben, werden die DB2-Quelle und das DB2-Ziel, die nicht in der Db2TypesFile aufgelistet sind, in den Db2Type umgewandelt. Wenn Sie keinen DB2-Subsystemtyp angeben, wird der standardmäßige DB2-Subsystemtyp verwendet. Standardwert ist LUW.
-Db2TypesFile -df	db2_types_file	Optional. Eine Eigenschaftendatei, die die PowerCenter DB2-Quelle und den Db2-Subsystemtyp enthält. Sie können eine Datei vom Typ Db2 verwenden, wenn die Db2-Quelle und das Db2-Ziel aus verschiedenen Subsystemen, wie z. B. LUW, z/OS oder i/OS, stammen. Sie können entweder Db2Type oder DB2TypesFile oder beides angeben. Wenn Sie sowohl Db2Type als auch Db2TypesFile für IBM DB2-Objekte angeben, werden die DB2-Quelle und das DB2-Ziel, die nicht in der Db2TypesFile aufgelistet sind, in den Db2Type umgewandelt. Wenn Sie den DB2-Subsystemtyp nicht angeben, wird der standardmäßige DB2-Subsystemtyp verwendet. Standardwert ist LUW.

Option	Argument	Beschreibung
- DefaultLookupConType -dl	default_lookup_con_type	Optional. Der für die Umwandlung verwendete Lookup-Verbindungstyp. Sie können entweder DefaultLookupConType oder LookupConTypesFile oder beides angeben. Wenn Sie sowohl DefaultLookupConType als auch LookupConTypesFile für die Lookup-Objekte angeben, werden die in der LookupConTypesFile nicht aufgelisteten Lookup-Umwandlungen in den DefaultLookupConType konvertiert.  Wenn Sie den DefaultLookupConType für ein Lookup-Objekt während der Umwandlung nicht angeben, wird der Standardverbindungstyp verwendet. Standardwert ist ODBC.
- LookupConTypesFile -lcf	lookup_connection_type_file	Optional. Eine Eigenschaftendatei, die die Lookup-Quelle und den Lookup-Verbindungstyp enthält. Sie können eine Lookup-Verbindungstypdatei verwenden, wenn die Lookup-Objekte aus verschiedenen Datenbanken, wie z. B. Oracle oder IBM DB2, stammen.  Sie können entweder DefaultLookupConType oder LookupConTypesFile oder beides angeben.  Wenn Sie beide Dateien für die Lookup-Objekte angeben, werden die nicht in LookupConTypesFile aufgelisteten Lookup-Umwandlungen in den DefaultLookupConType konvertiert.  Wenn Sie den DefaultLookupConType für ein Lookup-Objekt während der Umwandlung nicht angeben, wird der Standardverbindungstyp verwendet. Standardwert ist ODBC.
- ConvertOverrideprops -orprops	True False	Optional. Behält Überschreibungseigenschaften für die wiederverwendbare PowerCenter-Quelle, das Ziel sowie für Umwandlungen während der Konvertierung bei.  Der Befehl erstellt nicht wiederverwendbare Umwandlungen für PowerCenter-Umwandlungen mit Überschreibungseigenschaften. Er erstellt auch wiederverwendbare Datenobjekte für PowerCenter-Quellen und -Ziele mit Überschreibungseigenschaften.  Gültige Werte sind „True“ oder „False“.  Standardwert ist „True“.
-LogFile -lf	log_file	Optional. Pfad und Dateiname der Ausgabeprotokolldatei.  Standardwert ist „STDOUT“.

## genReuseReportFromPC

Erzeugt einen Bericht, in dem die Anzahl der PowerCenter-Mappings geschätzt wird, die im Modellrepository für eine native oder Hadoop-Umgebung wiederverwendet werden können. Sie können den Bericht als PDF- oder Excel-Datei generieren.

**Hinweis:** Wenn Sie den Bericht als Excel-Datei generieren, klicken Sie in der Statusleiste auf **Inhalt aktivieren**, um alle Tabellenblätter zu laden.

Stellen Sie vor dem Ausführen des Befehls „`infacmd ipc genReuseReportFromPC`“ sicher, dass Sie die folgenden Aufgaben ausführen:

- Konfigurieren Sie die erforderlichen Umgebungsvariablen für den Befehl „`pmrep`“.

- Wenn Sie eine Linux-Umgebung verwenden, gewähren Sie die Berechtigungen zum Lesen, Schreiben und Ausführen für jeden Versionsordner, der sich in folgendem Verzeichnis befindet: `<informatica server installation directory>/tools/pcutils`

Der Befehl „`infacmd ipc genReuseReportFromPC`“ verwendet die folgende Syntax:

```
genReuseReportFromPC
<-RepositoryName|-r> Pc_Repository_Name
<-HostName|-h> Pc_Domain_HostName
<-PortNumber|-o> Pc_Domain_PortNumber
[<-UserName|-n> Domain_UserName]
[<-Password|-x> Domain_Password]
[<-SecurityDomain|-s> Pc_Repository_Security_domain]
<-folderNames|-f> Pc_Folder_Names
<-SrcRelease|-srel> Pc_Release_version
[<-targetRelease|-trel> Target_Release_version]
[<-CodePage|-cp> Pc_Repository_code_page]
<-targetDir|-td> Target_Directory
<-authenticationType|-at> authentication_Type
[<-LogFile|-lf> Log_file_Name]
[<-Font> Font_to_use_for_PDF]
[<-ExecutionEnvironment|-execMode> Execution_Environment]
[<-BlockSize> Block_Size]
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd ipc genreusereportfrompc`“ beschrieben:

Option	Argument	Beschreibung
-RepositoryName -r	Pc_Repository_Name	Erforderlich. Der Name des PowerCenter-Repository.
-HostName -h	Pc_Domain_HostName	Erforderlich. Der Hostname des PowerCenter-Repositorys.
-PortNumber -o	Pc_Domain_PortNumber	Erforderlich. Die Portnummer des Gateway-Knotens.
-UserName -n	Domain_UserName	Optional. Benutzername der PowerCenter-Domäne. Wenn Sie keinen Benutzernamen eingeben, verwendet der Befehl den Wert in der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER.
Passwort -x	Domain_Password	Optional. Passwort für die PowerCenter-Domäne. Wenn Sie keinen Benutzernamen eingeben, verwendet der Befehl den Wert in der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD.



Option	Argument	Beschreibung
-SecurityDomain -s	Pc_Repository_Security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wenn Sie keine Sicherheitsdomäne eingeben, verwendet der Befehl den Wert in der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN. Sie können als Wert „Native“, „LDAP“ oder „SSO“ verwenden. Der Standardwert ist „Native“.
-folderNames -f	Pc_Folder_Names	Erforderlich. PowerCenter-Ordner, die die wiederzuverwendenden Objekte enthalten. Die Ordnernamen können Ausdrücke enthalten. Die Ordnernamen können * als Ausdrücke enthalten. <b>Hinweis:</b> Wenn Sie die Linux-Umgebung verwenden, dürfen Sie „\$“ nicht im Ordnernamen verwenden.
-SrcRelease -srel	Pc_Release-Version	Erforderlich. Die dem PowerCenter-Repository zugeordnete Release-Version. Geben Sie die Version im folgenden Format ein:  10.x.x  Geben Sie beispielsweise eine Version im folgenden Format ein:  10.2.0
-targetRelease -trel	Target_Release_version	Optional. Die dem Modellrepository zugeordnete Release-Version. Wenn Sie keine Version eingeben, verwendet der Befehl die Produktversion. Sie können Versionen ab 10.0.0 eingeben. Geben Sie die Version im folgenden Format ein:  10.x.x  Geben Sie beispielsweise eine Version im folgenden Format ein:  10.2.1
-CodePage -cp	Pc_Repository_code_page	Optional. Codepage des PowerCenter-Repository. Standardwert ist UTF-8.
-targetDir -td	Target_Directory	Erforderlich. Speicherort des Zielverzeichnisses auf dem Computer, auf dem der infacmd-Client und -Server ausgeführt werden. Sie müssen im Zielverzeichnisordner über Berechtigungen zum Lesen, Schreiben und Ausführen verfügen. Geben Sie beispielsweise den Speicherort des infacmd-Clients im folgenden Format ein:  installed_location_of_client\clients\DeveloperClient\infacmd  Geben Sie beispielsweise den Speicherort des infacmd-Servers im folgenden Format ein:  installed_location_of_server\isp\bin  <b>Hinweis:</b> Auf einem Linux-Computer können Sie „\$“ nicht im Namen des Zielverzeichnisses verwenden.
authenticationType -at	authentication_Type	Erforderlich. Der Typ der Benutzerauthentifizierung für die Domäne. Geben Sie einen der folgenden Werte ein: „LDAP“, „Native“ oder „Kerberos Single Sign On“.

Option	Argument	Beschreibung
-LogFile -lf	Log_file_Name	Optional. Name der generierten Protokolldatei. Wenn Sie keinen Namen eingeben, druckt der Befehl die Protokolle auf der Konsole. Verwendet den Wert von file_path/file_name.  Wenn Sie einen Dateinamen eingeben, wird die Protokolldatei mit demselben Namen im infacmd-Ordner angezeigt.  Wenn Sie einen Verzeichnispfad eingeben, der nicht gültig ist, wird die Protokolldatei mit dem Pfadnamen im infacmd-Ordner angezeigt. Wenn Sie beispielsweise „x“ als Verzeichnispfad eingeben, wird die Protokolldatei mit dem Namen „x“ im infacmd-Ordner angezeigt.
-Font	Font_to_use_for_PDF	Optional. Der Speicherort für die Schriftart-Datei mit Unicode-Zeichen im Bericht.
- ExecutionEnvironment -execMode	Execution_Environment	Optional. Die Laufzeit-Engine in der Hadoop-Umgebung. Der Bericht validiert Mappings basierend auf der von Ihnen gewählten Laufzeit-Engine. Sie können „Blaze“ oder „Hive“ als Wert verwenden. Wenn Sie keinen Wert eingeben, wird der Bericht für alle Engines ausgeführt und enthält nur die Engine mit den geringsten Fehlern.
-BlockSize	Block_Size	Optional. Die Anzahl der Mappings, für die der Befehl „infacmd ipc genReuseReportFromPC“ ausgeführt werden soll. Falls Sie keinen Wert eingeben, wird der Bericht ausgeführt und alle Mappings in den einzelnen Ordnern werden in einem Schritt konvertiert. Wenn der zum Ausführen des Befehls erforderliche Arbeitsspeicher nicht verfügbar ist, steuern Sie die Anzahl der Mappings mithilfe der Option -BlockSize, statt den Befehl für alle Mappings im Repository auszuführen.

## KAPITEL 21

# Infacmd isp-Befehlsreferenz

Das infacmd isp-Programm verwaltet die Informatica-Domäne, die Sicherheit und die PowerCenter-Anwendungsdienste. Sie können Informatica-Dienste mit infacmd isp-Befehlen aktivieren und deaktivieren.

Dieses Kapitel umfasst die Befehle, die Sie mit dem infacmd isp-Programm verwenden können.

## AddAlertUser

Abonniert Alarm-E-Mail-Nachrichten für einen Benutzer. Bevor Sie Alarme für einen Benutzer abonnieren können, müssen Sie die SMTP-Einstellungen für den ausgehende Mailserver konfigurieren. Sie können „infacmd isp AddAlertUser“ für alle Benutzer ausführen.

Wenn Sie Alarme abonnieren, erhalten Sie Domänen- und Dienstbenachrichtigungen per E-Mail für diejenigen Objekte, für die Sie Berechtigungen haben.

Der Befehl „infacmd isp AddAlertUser“ verwendet die folgende Syntax:

```
AddAlertUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

[<-SecurityDomain|-sdn> security_domain]

<-Password|-pd> password

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-AlertUser|-au> user_name
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddAlertUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.inf“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-AlertUser -au	user_name	Erforderlich. Name des Benutzers, für den Sie Alarme abonnieren möchten.

## VERWANDTE THEMEN:

- [“UpdateSMTPOptions” auf Seite 813](#)

# AddConnectionPermissions

Weist einem Benutzer oder einer Gruppe Verbindungsberechtigungen zu.

Der Befehl „infacmd isp AddConnectionPermissions“ verwendet die folgende Syntax:

```
AddConnectionPermissions  
  
<-DomainName|-dn> domain_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-SecurityDomain|-sdn> security_domain]  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]  
  
<<-RecipientUserName|-run> recipient_user_name|<RecipientGroupName|-rgn>  
recipient_group_name>  
  
<-RecipientSecurityDomain|-rsd> recipient_security_domain]  
  
<-ConnectionName|-cn> connection_name  
  
[<-Permission|-p> permission_READ|WRITE|EXECUTE|GRANT|ALL
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddConnectionPermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RecipientUserName -run	recipient_user_name	Erforderlich, wenn Sie den Gruppennamen des Empfängers nicht angeben. Name des Benutzers, dem die Verbindungsberechtigung zugewiesen ist.
-RecipientGroupName -rgn	recipient_group_name	Erforderlich, wenn Sie den Benutzernamen des Empfängers nicht angeben. Name der Gruppe, der die Verbindungsberechtigung zugewiesen ist.
-RecipientSecurityDomain -rsd	recipient_security_domain_name	Erforderlich, wenn der Empfänger zu einer LDAP-Sicherheitsdomäne gehört. Name der Sicherheitsdomäne, zu der der Empfänger gehört. Standardwert ist „Native“.

Option	Argument	Beschreibung
-ConnectionName -cn	connection_name_security_domain	Erforderlich. Name der Verbindung
-Permission -p	permission	Erforderlich. Typ der zuzuweisenden Berechtigung. Geben Sie mindestens einen der folgenden Werte durch Leerzeichen getrennt ein: <ul style="list-style-type: none"> <li>- READ</li> <li>- WRITE. Lesen und Schreiben</li> <li>- EXECUTE</li> <li>- GRANT. Lesen und Gewähren</li> <li>- ALL. Lesen, Schreiben, Ausführen, Gewähren</li> </ul>

## addCustomLDAPType

Fügt einen benutzerdefinierten LDAP-Typ hinzu, der einen LDAP-Verzeichnisdienst definiert, aus dem Sie Benutzer in eine LDAP-Sicherheitsdomäne importieren.

Der Befehl „`infacmd isp addCustomLDAPType`“ verwendet die folgende Syntax:

```
addCustomLDAPType
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-CustomLDAPTypeName|-lt> custom_LDAP_type_name
<-DisplayName|-dpn> display_name
<-Uid> uid
[<-GroupMembershipAttr|-gm> group_membership_attr]
[<-GroupDescriptionAttr|-gd> group_description_attr]
[<-UserSurnameAttr|-usn> user_surname_attr]
[<-UserGivenNameAttr|-ugn> user_given_name_attr]
[<-UserEmailAttr|-ue> user_email_attr]
[<-UserEnableAttr|-uen> user_enable_attr]
[<-UserTelephoneAttr|-utn> user_telephone_attr]
[<-UserDescriptionAttr|-ud> user_description_attr]
[<-CN> cn]
[<-FetchRangedAttr|-fr> fetch_ranged_attr]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp addCustomLDAPType“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.



Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-CustomLDAPTypeName -lt	Name des benutzerdefinierten LDAP-Typs	Erforderlich. Name des benutzerdefinierten LDAP-Typs.
-DisplayName -dpn	Anzeigenname	Erforderlich. Name des benutzerdefinierten LDAP-Typs, der im Administrator Tool angezeigt wird.
-Uid	uid	Erforderlich. Name des Attributs im LDAP-Verzeichnisdienst, das den eindeutigen Bezeichner (UID) enthält, den der Dienstmanager zum Identifizieren von Benutzern verwendet.
-GroupMembershipAttr -gm	Attribut „Gruppenmitgliedschaft“	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das Informationen zur Gruppenmitgliedschaft eines Benutzers enthält.
-GroupDescriptionAttr -gd	Attribut „Gruppenbeschreibung“	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das beschreibenden Text über die Gruppen im Verzeichnisdienst enthält.
-UserSurnameAttr -usn	Attribut „Nachname des Benutzers“	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das den Nachnamen eines Benutzers enthält.
-UserGivenNameAttr -ugn	Attribut „Vorname des Benutzers“	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das den Vornamen eines Benutzers enthält.
-GroupMembershipAttr -gm	LDAP_Group_Membership_Attribute	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das die Namen der Gruppen im Verzeichnisdienst enthält.
--UserEmailAttr -ue	Attribut „E-Mail des Benutzers“	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das die E-Mail-Adresse eines Benutzers enthält.
-UserEnableAttr -uen	Attribut „Benutzeraktivierung“	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das enthält
-UserTelephoneAttr -utn	Attribut „Telefonnummer des Benutzers“	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das die Telefonnummer eines Benutzers enthält.
-UserDescriptionAttr -ud	Attribut „Benutzerbeschreibung“	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das eine Beschreibung des Benutzers enthält.

Option	Argument	Beschreibung
-CN	cn	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das das Attribut mit dem vollständigen Namen oder dem gebräuchlichen Namen eines Benutzers enthält.
- FetchRangedAttr -fr	Attribut „Bereich abrufen“	Optional. Auf true festlegen, um alle Werte abzurufen, die in Attributen mit mehreren Werten enthalten sind. Verwenden Sie diese Option nur für Microsoft Active Directory.

## AddDomainLink

Fügt einer Domäne einen Link hinzu. Zeichnet Verbindungseigenschaften für eine Remotedomäne oder eine verknüpfte Domäne auf, sodass Sie Repository-Metadaten zwischen der lokalen Domäne und der verknüpften Domäne austauschen können.

Möglicherweise möchten Sie einen Link zu einer Domäne hinzufügen, wenn Sie auf einen PowerCenter-Repository-Dienst in dieser Domäne zugreifen müssen.

Sie können einen Link zu einer anderen Informatica-Domäne hinzufügen, wenn Sie ein lokales Repository mit einem globalen Repository in einer anderen Informatica-Domäne registrieren oder die Registrierung aufheben.

Der Befehl „infacmd isp AddDomainLink“ verwendet die folgende Syntax:

```
AddDomainLink
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LinkedDomainName|-ld> linked_domain_name
<-DomainLink|-dl> domain_host1:port domain_host2:port...
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddDomainLink“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der lokalen Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeitraum in Sekunden, in dem infacmd versucht, eine Verbindung zur lokalen Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LinkedDomainName -ld	linked_domain_name	Erforderlich. Name der Domäne, mit der Sie eine Verbindung herstellen möchten.
-DomainLink -dl	gateway_host1:port gateway_host2:port ...	Erforderlich. Die Hostnamen und Portnummern für die Gateway-Knoten in der verknüpften Domäne.

## AddDomainNode

Fügt der Domäne einen Knoten hinzu. Bevor Sie den Knoten starten können, müssen Sie ihn definieren, indem Sie infasetup DefineGatewayNode oder DefineWorkerNode auf dem Knoten ausführen.

Der Befehl „infacmd isp AddDomainNode“ verwendet die folgende Syntax:

```
AddDomainNode
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
[<-FolderPath|-fp> full_folder_path]
[<-EnableServiceRole|-esr> true|false]
[<-EnableComputeRole|-ecr> true|false]
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddDomainNode“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-NodeName -nn	node_name	Erforderlich. Name des Knotens, den Sie der Domäne hinzufügen möchten.
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, dem Sie den Knoten hinzufügen möchten. Folgendes Format ist erforderlich:  <i>/parent_folder/child_folder</i> Standardwert ist „/“ (die Domäne).
-EnableServiceRole -esr	true   false	Optional. Aktiviert die Dienstrolle auf dem Knoten. Bei „True“ können Anwendungsdienste auf dem Knoten ausgeführt werden. Bei „False“ können Anwendungsdienste nicht auf dem Knoten ausgeführt werden. Legen Sie den Befehl nur auf „False“ fest, wenn der Knoten einem Datenintegrationsdienst-Gitter zugewiesen ist und Sie den Knoten für ausgeführte Mappings dedizieren möchten. Standardwert ist „True“.
-EnableComputeRole -esr	true   false	Optional. Aktiviert die Berechnungsrolle auf dem Knoten. Bei „True“ kann der Knoten Berechnungen durchführen, die von Remote-Anwendungsdiensten angefragt werden. Bei „False“ kann der Knoten keine von Remote-Anwendungsdiensten angefragten Berechnungen durchführen. Für einen Knoten ist die Berechnungsrolle erforderlich, wenn der Datenintegrationsdienst Jobs auf diesem Knoten ausführt. Wenn der Datenintegrationsdienst auf diesem Knoten keine Jobs ausführt, können Sie die Berechnungsrolle deaktivieren. Eine aktivierte oder deaktiverte Berechnungsrolle hat allerdings keine Auswirkungen auf die Leistung. Standardwert ist „True“.

## AddGroupPrivilege

Weist einer Gruppe in der Domäne eine Berechtigung zu. Sie können einer Gruppe Berechtigungen für die Domäne zuweisen. Sie können ebenfalls Gruppenberechtigungen für jeden Anwendungsdienst in der Domäne zuweisen.

Der Befehl „infacmd isp AddGroupPrivilege“ verwendet die folgende Syntax:

```
AddGroupPrivilege
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-Gateway|-hp> gateway_host1:port gateway_host2:port...
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GroupName|-gn> group_name
```

[<-GroupSecurityDomain|-gsf> group\_security\_domain]

<-ServiceName|-sn> service\_name

<-PrivilegePath|-pp> path\_of\_privilege

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddGroupPrivilege“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Native“.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-GroupName -gn	group_name	Erforderlich. Name der Gruppe, der Sie die Berechtigung zuweisen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-GroupSecurityDomain -gsf	group_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der die Gruppe gehört, der Sie die Berechtigung zuweisen. Standardwert ist „Native“.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, für die bzw. den Sie Berechtigungen anzeigen möchten.
-PrivilegePath -pp	path_of_privilege	Erforderlich. Vollqualifizierter Name der Berechtigung, die Sie der Gruppe zuweisen möchten. Ein vollqualifizierter Name enthält den Namen der Berechtigungsgruppe und den Namen der Berechtigung. Ein vollqualifizierter Berechtigungsname für den Repository-Dienst ist z. B. „folder/create“. Wenn der Berechtigungsname Leerzeichen enthält, setzen Sie den Pfad in Anführungszeichen wie folgt:  "Runtime Objects/Monitor/Execute/Manage Execution"  Wenn der Berechtigungsname das Sonderzeichen „/" enthält, fügen Sie das Escape-Zeichen „\" davor folgendermaßen ein:  "Model/View Model/Export\\/Import Models"

## addLDAPConnectivity

Konfiguriert eine Verbindung zu einem LDAP-Server. Wenn Sie eine Sicherheitsdomäne angeben, importiert der Dienstmanager Benutzer und Gruppen aus dem LDAP-Verzeichnisdienst in die Sicherheitsdomäne.

Der Befehl „infacmd isp addLDAPConnectivity“ verwendet die folgende Syntax:

```
addLDAPConnectivity
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LDAPAddress|-la> ldap_server_address
[<-LDAPPrincipal|-lp> ldap_principal]
[<-LDAPCredential|-lc> ldap_credential]
[<-UseSSL|-us> use_ssl]
```



```
[<-TrustLDAPCertificate|-tc> trust_ldap_certificate]

<-LDAPType|-lt> ldap_types=MicrosoftActiveDirectory, MicrosoftAzureActiveDirectory,
SunJavaSystemDirectory, NovellE-Directory, IBMTivoliDirectory, OpenLDAP,
OracleDirectoryServerODSEE, OracleUnifiedDirectory, <Custom LDAP Type Name>

[<-MaxSecurityDomainSize|-ms> Max_Security_Domain_size]

[<-GroupMembershipAttr|-gm> LDAP_Group_Membership_Attribute]

[<-LDAPNotCaseSensitive|-lnc> ldap_not_case_sensitive]

<-LDAPHostConfigurationName|-lcn> LDAP_host_configuration_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp addLDAPConnectivity“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	<p>Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.</p>
-LDAPAddress -la	ldap_server_address	<p>Erforderlich. Hostname und Portnummer für den Computer, auf dem der LDAP-Verzeichnisdienst gehostet wird. In der Regel weist der LDAP-Server die Portnummer 389 auf. Wenn der LDAP-Server SSL verwendet, lautet dessen Portnummer 636.</p>
-LDAPPrincipal -lp	ldap_principal	<p>Optional. Distinguished Name (DN) für den Prinzipal-Benutzer. Lassen Sie diese Option aus, um sich als anonymer Benutzer anzumelden.</p> <p>Weitere Informationen finden Sie in der Dokumentation für den LDAP-Verzeichnisdienst.</p>
-LDAPCredential -lc	ldap_credential	<p>Optional. Passwort für den Prinzipal-Benutzer. Sie können ein Passwort mit der Option -lc oder der Umgebungsvariablen INFA_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -lc festgelegte Passwort Vorrang.</p> <p>Lassen Sie diese Option aus, um sich als anonymer Benutzer anzumelden.</p>
-UseSSL -us	use_ssl	<p>Optional. Wenn Sie die Option einbeziehen, verwendet der LDAP-Verzeichnisdienst das SSL-Protokoll (Secure Socket Layer).</p>

Option	Argument	Beschreibung
-TrustLDAPCertificate -tc	trust_ldap_certificate	Optional. Wenn Sie die Option einbeziehen, stellt PowerCenter eine Verbindung zum LDAP-Server ohne Überprüfung des SSL-Zertifikats aus.  Wenn Sie die Option nicht einbeziehen, stellt PowerCenter vor dem Herstellen einer Verbindung zum LDAP-Server sicher, dass das SSL-Zertifikat von einer Zertifizierungsstelle signiert ist.
-LDAPType -lt	ldap_types=value	Erforderlich. Typ des LDAP-Verzeichnisdiensts. Verzeichnisdienste umfassen: <ul style="list-style-type: none"> <li>- MicrosoftActiveDirectory</li> <li>- Microsoft Azure Active Directory</li> <li>- SunJavaSystemDirectory</li> <li>- NovellE-Directory</li> <li>- IBMTivoliDirectory</li> <li>- OpenLDAP</li> <li>- Oracle Directory Server (ODSEE)</li> <li>- Oracle Unified Directory</li> </ul> Wenn Sie einen benutzerdefinierten LDAP-Verzeichnisdienst verwenden, geben Sie den Namen des Diensts an.
-MaxSecurityDomainSize -ms	Max_Security_Domain_size	Optional. Maximale Anzahl an Benutzerkonten zum Importieren in eine Sicherheitsdomäne. Standardwert ist „1000“.
-GroupMembershipAttr -gm	LDAP_Group_Membership_Attribute	Optional. Name des Attributs, das Informationen zur Gruppenmitgliedschaft eines Benutzers enthält.
-LDAPNotCaseSensitive -lnc	LDAP_Not_Case_Sensitive	Optional. Gibt an, dass die Benutzernamen aus dem LDAP-Verzeichnisdienst der Groß-/Kleinschreibung nicht unterliegen. Standardwert ist „false“.
LDAPHostConfigurationName -lcn	LDAP-Hostkonfigurationsname	Erforderlich. Der Name der LDAP-Konfiguration.

## AddLicense

Fügt der Domäne eine Lizenz hinzu. Nachdem Sie eine Lizenz hinzugefügt haben, können Sie sie mit dem AssignLicence-Befehl zu einem Anwendungsdienst zuweisen. Sie müssen einem Dienst eine Lizenz zuweisen, bevor Sie den Dienst verwenden können.

Der Befehl „infacmd isp AddLicense“ verwendet die folgende Syntax:

```
AddLicense
<-DomainName|-dn> domain_name
```

```

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> securitydomain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-LicenseName|-ln> license_name

<-LicenseKeyFile|-lf> license_key_file

[<-FolderPath|-fp> full_folder_path]

```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddLicense“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz. Der Name unterliegt nicht der Groß-/ Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten:  / * ? < > "
-LicenseKeyFile -lf	license_key_file	Erforderlich. Pfad zur Lizenzschlüsseldatei.
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, dem Sie die Lizenz hinzufügen möchten. Folgendes Format ist erforderlich:  /parent_folder/child_folder Standardwert ist „/“ (die Domäne).

## AddNamespace

Erstellt eine LDAP-Sicherheitsdomäne und setzt die Filter so, dass nach Benutzern oder Gruppen im Verzeichnisdienst gesucht wird. Erstellt die LDAP-Sicherheitsdomäne, wenn die Informatica-Domäne LDAP oder die Kerberos-Authentifizierung verwendet.

Der Befehl „infacmd isp AddNamespace“ verwendet die folgende Syntax:

```
AddNamespace
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NameSpace|-ns> namespace
[<-UserSearchBase|-usb> usersearchbase]
[<-UserFilter|-uf> userfilter]
```

[<-GroupSearchBase|-gsb> groupsearchbase]

[<-GroupFilter|-gf> groupfilter]

<-LDAPHostConfigurationName|-lcn> LDAP\_host\_configuration\_name

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddNamespace“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Sie können einen Wert für -sdn angeben oder den Standardwert basierend auf dem Authentifizierungsmodus verwenden: <ul style="list-style-type: none"><li>- Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Standardwert ist „Nativ“. Zum Arbeiten mit der LDAP-Authentifizierung müssen Sie den Wert für -sdn angeben.</li><li>- Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Standardwert ist „Native“ für native Authentifizierung. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</li></ul>

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn Sie die Umgebungsvariable nicht angeben, wird der Standardwert von 180 Sekunden verwendet.
-NameSpace -ns	namespace	Erforderlich. Name der LDAP- oder Kerberos-Sicherheitsdomäne, die Sie hinzufügen möchten. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf weder Leerzeichen noch folgende Sonderzeichen enthalten: , + / < > @ ; \ % ? Der Name darf nicht länger als 128 Zeichen sein. Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Sie können keine anderen Leerzeichen verwenden.
-UserSearchBase -usb	usersearchbase	Distinguished Name (DN) des Eintrags, der als Ausgangspunkt für die Suche nach Benutzernamen im LDAP-Verzeichnisdienst dient. Der LDAP-Verzeichnisdienst sucht nach einem Objekt im Verzeichnis entsprechend dem Pfad im Distinguished Name des Objekts. Beispiel: In Microsoft Active Directory könnte der Distinguished Name des Benutzers cn=UserName,ou=OrganizationalUnit,dc=DomainName lauten. Die Reihe der durch dc=DomainName benannten relativen Distinguished Names kennzeichnet die DNS-Domäne des Objekts.
-UserFilter -uf	userfilter	Ein LDAP-Abfragestring, der die Suchkriterien für die Suche nach Benutzern im Verzeichnisdienst festlegt. Der Filter kann Attributtypen, Assertionswerte und Abgleichkriterien angeben. Beispiel: Der Filter (objectclass=*) sucht alle Objekte. Der Filter (&(objectClass=user)!(cn=susan)) sucht alle Benutzerobjekte außer „susan“. Weitere Informationen über Suchfilter finden Sie in der Dokumentation für den LDAP-Verzeichnisdienst:
-GroupSearchBase -gsb	groupsearchbase	Distinguished Name (DN) des Eintrags, der als Ausgangspunkt für die Suche nach Gruppennamen im LDAP-Verzeichnisdienst dient.
-GroupFilter -gf	groupfilter	Ein LDAP-Abfragestring, der die Kriterien für die Suche nach Gruppen im Verzeichnisdienst festlegt.
-LDAPHostConfigurationName -lcn	LDAP-Hostkonfigurationsname	Erforderlich. Der Name der LDAP-Konfiguration, die der Sicherheitsdomäne zugeordnet ist.

# AddNodeResource

Fügt eine benutzerdefinierte Ressource oder eine Dateiverzeichnisressource zu einem Knoten hinzu.

Wenn ein PowerCenter-Integrationsdienst in einem Gitter ausgeführt wird, kann der Load Balancer Ressourcen verwenden, um Sitzungs-, Befehls- und vordefinierte Event-Wait-Aufgaben zu verteilen. Wenn der PowerCenter-Integrationsdienst für die Überprüfung von Ressourcen konfiguriert ist, verteilt der Load Balancer Aufgaben an Knoten, auf denen Ressourcen hinzugefügt und aktiviert werden.

Der Befehl „infacmd isp AddNodeResource“ verwendet die folgende Syntax:

```
AddNodeResource

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

[<-ResourceCategory|-rc> resource_category ("PCIS", "DIS")]

<-ResourceType|-rt> resource_type("Custom", "File Directory")

<-ResourceName|-rn> resource_name

[<-ResourceValue|-rv> resource_value]
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddNodeResource“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.



Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem Sie eine Ressource hinzufügen möchten.
-ResourceCategory -rc	resource_category	Optional. Kategorie der Ressource. Gültige Kategorien umfassen: - PCIS. Ressource für den PowerCenter-Integrationsdienst. - DIS. Für zukünftige Verwendung reserviert. Standardwert ist PCIS.
-ResourceType -rt	resource_type	Erforderlich. Typ der Ressource. Gültige Typen umfassen: - Benutzerdefiniert - Dateiverzeichnis

Option	Argument	Beschreibung
-ResourceName -rn	resource_name	Erforderlich. Name der Ressource. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten:  \ / * ? < > "   \$
-ResourceValue -rv	resource_value	Optional. Für zukünftige Verwendung reserviert.

## AddRolePrivilege

Weist einer Rolle in der Domäne eine Berechtigung zu. Sie können einer Rolle Berechtigungen für die Domäne zuweisen. Sie können ebenfalls Rollenberechtigungen für jeden Anwendungsdienst in der Domäne zuweisen.

Der Befehl „infacmd isp AddRolePrivilege“ verwendet die folgende Syntax:

```
AddRolePrivilege
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-RoleName|-rn> role_name
<-ServiceType|-st> service_type AS|CMS|DIS|DOMAIN|LDM|MM|MRS|RS|SATS|SCH|TDM|TDW
<-PrivilegePath|-pp> path_of_privilege
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddRolePrivilege“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-RoleName -rn	role_name	Erforderlich. Name der Rolle, der Sie die Berechtigung zuweisen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-ServiceType -st	service_type	Erforderlich. Domäne oder Anwendungsdiensttyp, der bzw. dem Sie die Berechtigung für die Rolle zuweisen. Zu den Diensttypen gehören: <ul style="list-style-type: none"> <li>- AS. Analyst-Dienst</li> <li>- CMS. Content-Managementdienst</li> <li>- CS. Katalogdienst</li> <li>- DIS. Datenintegrationsdienst</li> <li>- DOMAIN. Domäne</li> <li>- MM. Metadata Manager-Dienst</li> <li>- MRS. Modellrepository-Dienst</li> <li>- RS. PowerCenter-Repository-Dienst</li> <li>- TDM. Test Data Manager-Dienst</li> <li>- TDW. Test Data Warehouse-Dienst</li> <li>- SATS. Secure At Source-Dienst.</li> <li>- SCH. Scheduler-Dienst</li> </ul>
-PrivilegePath -pp	path_of_privilege	Erforderlich. Vollqualifizierter Name der Berechtigung, die Sie der Gruppe zuweisen möchten. Ein vollqualifizierter Name enthält den Namen der Berechtigungsgruppe und den Namen der Berechtigung. Ein vollqualifizierter Berechtigungsname für den Repository-Dienst ist z. B. „folder/create“. Wenn der Berechtigungsname Leerzeichen enthält, setzen Sie den Pfad wie folgt in Anführungszeichen:  <pre>"Runtime Objects/Monitor/Execute/Manage Execution"</pre> Wenn der Berechtigungsname das Sonderzeichen „/“ enthält, fügen Sie das Escape-Zeichen „\“ davor folgendermaßen ein:  <pre>"Model/View Model/Export\Import Models"</pre>

## AddServiceLevel

Fügt eine Dienstebene hinzu.

Dienstebenen geben eine Priorität unter den Aufgaben an, die darauf warten, versendet zu werden. Sie können unterschiedliche Dienstebenen erstellen, die ein Aufgabenentwickler Arbeitsabläufen zuweisen kann.

Jede Dienstebene, die Sie erstellen, hat einen Namen, eine Dispatch-Priorität und eine maximale Dispatch-Wartezeit. Die Dispatch-Priorität ist eine Zahl, mit der die Priorität für den Versand angegeben ist. Der Load Balancer versendet zuerst Aufgaben mit einer hohen Priorität, dann Aufgaben mit niedriger Priorität. Die maximale Dispatch-Wartezeit gibt an, wie lange der Load Balancer wartet, bevor die Dispatch-Priorität für eine Aufgabe in die höchste Priorität geändert wird.

Der Befehl „infacmd isp AddServiceLevel“ verwendet die folgende Syntax:

```
AddServiceLevel
<-DomainName|-dn> domain_name
```

```

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> securitydomain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceLevelName|-ln> service_level_name

<-ServiceLevel|-sl> option_name=value ...

```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddServiceLevel“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domännennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domännennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomännennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceLevelName -ln	service_level_name	Erforderlich. Name der Dienstebene.
-ServiceLevel -sl	option_name=value	Erforderlich. Die Eigenschaften der Dienstebene. Sie können die folgenden Eigenschaften festlegen: <ul style="list-style-type: none"> <li>- DispatchPriority. Die anfängliche Priorität für den Versand. Kleinere Zahlen haben höhere Priorität. Priorität 1 ist die höchste Priorität. Standardwert ist „5“.</li> <li>- MaxDispatchWaitTime. Der Zeitraum in Sekunden, bevor der Load Balancer die Dispatch-Priorität für eine Aufgabe in die höchste Priorität ändert. Standardwert ist „1800“.</li> </ul>

## AddUserPrivilege

Weist einem Benutzer in der Domäne eine Berechtigung zu. Sie können ebenfalls Benutzerberechtigungen für jeden Anwendungsdienst in der Domäne zuweisen.

Der Befehl „infacmd isp AddUserPrivilege“ verwendet die folgende Syntax:

```
AddUserPrivilege
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_Name
[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
<-ServiceName|-sn> service_name
<-PrivilegePath|-pp> path_of_privilege
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddUserPrivilege“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_name	Erforderlich. Benutzerkonto, dem Sie die Berechtigung zuweisen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, dem Sie die Berechtigung zuweisen. Standardwert ist „Native“.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, für die bzw. den Sie Berechtigungen anzeigen möchten.
-PrivilegePath -pp	path_of_privilege	Erforderlich. Vollqualifizierter Name der Berechtigung, die Sie der Gruppe zuweisen möchten. Ein vollqualifizierter Name enthält den Namen der Berechtigungsgruppe und den Namen der Berechtigung. Ein vollqualifizierter Berechtigungsname für den Repository-Dienst ist z. B. „folder/create“. Wenn der Berechtigungsname Leerzeichen enthält, setzen Sie den Pfad wie folgt in Anführungszeichen:  "Runtime Objects/Monitor/Execute/Manage Execution"  Wenn der Berechtigungsname das Sonderzeichen „/“ enthält, fügen Sie das Escape-Zeichen „\“ davor folgendermaßen ein:  "Model/View Model/Export\ /Import Models"

## AddUserToGroup

Fügt einer nativen Gruppe in der Domäne einen nativen oder LDAP-Benutzer hinzu. Der Benutzer erbt alle Berechtigungen, die mit Gruppe verbunden sind.

Der Befehl „infacmd isp AddUserToGroup“ verwendet die folgende Syntax:

```
AddUserToGroup
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
```



```

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_Name

[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]

<-GroupName|-gn> group_name

```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddUserToGroup“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_Name	Erforderlich. Name des Benutzers, den Sie hinzufügen möchten.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, den Sie hinzufügen möchten. Standardwert ist „Native“.
-GroupName -gn	group_name	Erforderlich. Name der Gruppe, der Sie den Benutzer hinzufügen möchten.

## AssignDefaultOSProfile

Weist ein Standardbetriebssystemprofil einem Benutzer oder einer Gruppe zu.

Der Befehl „infacmd isp AssignDefaultOSProfile“ verwendet die folgende Syntax:

```
AssignDefaultOSProfile
<-DomainName|-dn> domain_name
```

```

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-OSProfileName|-on> OSProfile_name

<-RecipientName|-nm> recipient_name

<-RecipientSecurityDomain|-ns> security_domain_of_recipient

<-RecipientType|-ty> recipient_type

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp AssignDefaultOSProfile“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-OSProfileName -on	OSProfile_name	Erforderlich. Name des Betriebssystemprofils. Der Name des Betriebssystemprofils kann bis zu 80 Zeichen enthalten. Er darf weder Leerzeichen noch die folgenden Sonderzeichen enthalten: % * + \ / ? ; < >
-RecipientName -nm	recipient_name	Erforderlich. Benutzer- oder Gruppenname, der dem Standardbetriebssystemprofil zugewiesen wird.

Option	Argument	Beschreibung
-RecipientSecurityDomain -ns	security_domain_of_recipient	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, zu der der Benutzer gehört.
-RecipientType -ty	recipient_type	Erforderlich. Geben Sie an, ob das Standardbetriebssystemprofil einem Benutzer oder einer Gruppe zugewiesen werden soll. Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- Useridentity</li> <li>- Groupidentity</li> </ul>

## AssignedToLicense

Listet die Dienste auf, die einer Lizenz zugewiesen sind. Sie können die Dienste auflisten, die einer Lizenz aktuell zugewiesen sind.

Der Befehl „infacmd isp AssignedToLicense“ verwendet die folgende Syntax:

```
AssignedToLicense
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LicenseName|-ln> license_name
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AssignedToLicense“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz.

# AssignGroupPermission

Weist einem Objekt eine Gruppenberechtigung zu.

Mit Berechtigungen kann eine Gruppe auf Objekte in einer Domäne zugreifen. Objekte beinhalten die Domäne, Ordner, Knoten, Gitter, Lizenzen und Anwendungsdienste. Wenn Sie beispielsweise eine Gruppenberechtigung einem Ordner zuweisen, erbt die Gruppe die Berechtigung für alle Objekte in diesem Ordner.

Der Befehl „infacmd isp AssignGroupPermission“ verwendet die folgende Syntax:

```
AssignGroupPermission
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingGroup|-eg> existing_group_name
[<-GroupSecurityDomain|-gsf> group_security_domain]
<-ObjectName|-on> object_name
<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AssignGroupPermission“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingGroup -eg	existing_group_name	Erforderlich. Name der Gruppe, der Sie eine Berechtigung für ein Objekt zuweisen möchten.
-GroupSecurityDomain -gsf	group_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der die Gruppe gehört, der Sie eine Berechtigung zuweisen möchten. Standardwert ist „Native“.

Option	Argument	Beschreibung
-ObjectName -on	object_name	Erforderlich. Name des Objekts, dem Sie die Gruppenzugriffsberechtigung zuweisen möchten.
-ObjectType -ot	object_type_SERVICE_LICENSE_NODE_GRID_FOLDERR_OSPROFILE	Erforderlich. Typ des Objekts Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- Dienst</li> <li>- Lizenz</li> <li>- Knoten</li> <li>- Gitter</li> <li>- Folder</li> <li>- OSPprofile</li> </ul>

## AssignISToMMService

Weist den zugeordneten PowerCenter-Integrationsdienst einem Metadata Manager-Dienst zu.

Der Befehl „infacmd isp AssignISToMMService“ verwendet die folgende Syntax:

```
AssignISToMMService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> securitydomain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-IntegrationService|-is> integration_service_name
[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]
<-RepositoryUser|-ru> repository_user
<-RepositoryPassword|-rp> repository_password
```



In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AssignISToMMService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Metadata Manager-Diensts, dem Sie den Integrationsdienst zuweisen möchten.
-IntegrationService -is	integration_service_name	Erforderlich. Name des PowerCenter-Integrationsdiensts, den Sie dem Metadata Manager-Dienst zuweisen möchten.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung oder Kerberos-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der PowerCenter-Repository-Benutzer gehört.  Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn Sie diese Option nicht festlegen, setzt der Befehl die Sicherheitsdomäne des Repository-Benutzers auf die in der Option -sdn angegebene Sicherheitsdomäne.
-RepositoryUser -ru	repository_user	Erforderlich. Name des PowerCenter-Repository-Benutzers.
-RepositoryPassword -rp	repository_password	Erforderlich. Passwort für den PowerCenter-Repository-Benutzer. Benutzerpasswort. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -rp festgelegte Passwort Vorrang.

## AssignLicense

Weist einem Anwendungsdienst eine Lizenz zu. Sie müssen einem Anwendungsdienst eine Lizenz zuweisen, bevor Sie den Dienst aktivieren können.

**Hinweis:** Sie können einem Dienst keine Lizenz zuweisen, wenn der Dienst einer anderen Lizenz zugeordnet ist. Um einem Dienst eine andere Lizenz zuzuweisen, entfernen Sie mit dem Befehl „RemoveLicense“ die vorhandene Lizenz aus dem Dienst und weisen dem Dienst dann die neue Lizenz zu.

Der Befehl „infacmd isp AssignLicense“ verwendet die folgende Syntax:

```
AssignLicense
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LicenseName|-ln> license_name
<-ServiceNames|-sn> service1_name service2_name ...
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AssignLicense“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz, die Sie einem Dienst zuweisen möchten.
-ServiceNames -sn	service_name1 service_name2 ...	Erforderlich. Namen der Dienste, für die Sie eine Lizenz zuweisen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen. Starten Sie den Dienst neu, um die Änderungen anzuwenden.

## AssignRoleToGroup

Weist eine Rolle zu einer Gruppe für eine Domäne oder einen Anwendungsdienst zu.

Der Befehl „`infacmd isp AssignRoleToGroup`“ verwendet die folgende Syntax:

```
AssignRoleToGroup
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GroupName|-gn> group_name
[<-GroupSecurityDomain|-gsf> group_security_domain]
<-RoleName|-rn> role_name
<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AssignRoleToGroup“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infra“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-GroupName -gn	group_name	Erforderlich. Name der Gruppe, der Sie die Rolle zuweisen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-GroupSecurityDomain -gsf	group_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der die Gruppe gehört, der Sie die Rolle zuweisen. Standardwert ist „Native“.
-RoleName -rn	role_name	Erforderlich. Name der Rolle, die Sie einer Gruppe zuweisen möchten.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, für die bzw. den Sie die Rolle zuweisen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

## AssignRoleToUser

Weist eine Rolle zu einem Benutzer für eine Domäne oder einen Anwendungsdienst zu.

Der Befehl „`infacmd isp AssignRoleToUser`“ verwendet die folgende Syntax:

```
AssignRoleToUser
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_Name
[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
<-RoleName|-rn> role_name
<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AssignRoleToUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_Name	Erforderlich. Benutzerkonto, dem Sie die Rolle zuweisen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, dem Sie die Rolle zuweisen. Standardwert ist „Native“.
-RoleName -rn	role_name	Erforderlich. Name der Rolle, die Sie dem Benutzer zuweisen möchten.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, für die bzw. den Sie die Rolle zuweisen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

## AssignRSToWSHubService

Verbindet ein PowerCenter-Repository mit einem Webdienst-Hub in der Domäne.

Der Befehl „infacmd isp AssignRSToWSHubService“ verwendet die folgende Syntax:

```
AssignRSToWSHubService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-NodeName|-nn> node_name
<-RepositoryService|-rs> repository_service_name
<-RepositoryUser|-ru> user
```



```
<-RepositoryPassword|-rp> password
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AssignRSToWSHubService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Webdienst-Hubs, dem Sie ein Repository zuordnen möchten.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Webdienst-Hub-Prozess ausgeführt werden soll. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, gibt diese Option den Namen des primären Knotens an.
-RepositoryService -rs	repository_service_name	Erforderlich. Name des PowerCenter-Repository-Diensts, von dem der Webdienst-Hub abhängig ist.  Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryUser -ru	user	Erforderlich. Benutzername zum Herstellen einer Verbindung zum Repository.  Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryPassword -rp	Passwort	Erforderlich. Benutzerpasswort. Benutzerpasswort. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -rp festgelegte Passwort Vorrang.

## AssignUserPermission

Weist einem Objekt eine Benutzerberechtigung zu.

Mit Berechtigungen kann ein Benutzer auf Objekte in einer Domäne zugreifen. Objekte beinhalten die Domäne, Ordner, Knoten, Gitter, Lizenzen und Anwendungsdienste. Wenn Sie beispielsweise eine Benutzerberechtigung einem Ordner zuweisen, erbt der Benutzer die Berechtigung für alle Objekte in diesem Ordner.

Der Befehl „infacmd isp AssignUserPermission“ verwendet die folgende Syntax:

```
AssignUserPermission
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
```

```

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_name

[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]

<-ObjectName|-on> object_name

<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE

```

In der folgenden Tabelle werden Optionen und Argumente für „*infacmd isp AssignUserPermission*“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert.
-ExistingUserName -eu	existing_user_name	Erforderlich. Name des Benutzers, dem Sie eine Berechtigung für ein Objekt zuweisen möchten.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, dem Sie eine Berechtigung zuweisen möchten. Standardwert ist „Native“.
-ObjectName -on	object_name	Erforderlich. Name des Objekts, dem Sie die Benutzerzugriffsberechtigung zuweisen möchten.
-ObjectType -ot	object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE	<p>Erforderlich. Typ des Objekts</p> <p>Geben Sie einen der folgenden Werte ein:</p> <ul style="list-style-type: none"> <li>- Dienst</li> <li>- Lizenz</li> <li>- Knoten</li> <li>- Gitter</li> <li>- Folder</li> <li>- OSProfile</li> </ul>

# ConvertLogFile

Wandelt binäre Protokolldateien in Textdateien, XML-Dateien oder auf dem Bildschirm lesbaren Text um.

Der infacmd isp ConvertLogFile-Befehl verwendet die folgende Syntax:

```
ConvertLogFile  
  
<-InputFile|-in> input_file_name  
  
[<-Format|-fm> format_TEXT_XML]  
  
[<-OutputFile|-lo> output_file_name]
```

In der folgenden Tabelle werden infacmd isp ConvertLogFile-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-InputFile -in	input_file_name	Erforderlich. Name und Pfad für die Protokolldatei, die Sie umwandeln möchten.  Standardmäßig schreibt der Service Manager Protokolldateien in das Verzeichnis "server\infa_shared\log" auf dem Master-Gateway-Knoten.
-Format -fm	format	Optional. Format der Ausgabedatei. Gültige Typen umfassen: - Text - XML  Wenn Sie kein Format angeben, verwendet infacmd Textformat mit einer Zeilenlänge von 80 Zeichen.
-OutputFile -lo	output_file_name	Optional. Name und Dateipfad für die Ausgabedatei.  Wenn Sie keinen Ausgabedateinamen angeben, zeigt infacmd die Protokollereignisse auf dem Bildschirm an.

# convertUserActivityLogFile

Wandelt eine mit dem getUserActivityLog-Befehl abgerufene binäre Benutzeraktivitäts-Protokolldatei in Text- oder XML-Format um.

Der infacmd isp convertUserActivityLogFile-Befehl verwendet die folgende Syntax:

```
convertUserActivityLogFile  
  
<-InputFile|-in> input_file_name  
  
[<-Format|-fm> format_TEXT_XML]  
  
[<-OutputFile|-lo> output_file_name]
```

In der folgenden Tabelle werden infacmd isp convertUserActivityLogFile-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-InputFile -in	input_file_name	Erforderlich. Name der zu konvertierenden Protokolldatei.
-Format -fm	format_TEXT_XML	Optional. Format der Ausgabedatei. Gültige Formate umfassen: - Text - XML Der Standardwert lautet „Text“.
-OutputFile -lo	output_file_name	Optional. Name der Ausgabedatei. Wenn Sie keinen Ausgabedateinamen angeben, zeigt der Befehl das Protokoll in der Befehlszeile an.

## CreateConnection

Definiert eine Verbindung und die Verbindungsoptionen.

Führen Sie infacmd isp ListConnectionOptions aus, um Verbindungsoptionen für eine vorhandene Verbindung aufzulisten.

Der Befehl „infacmd isp CreateConnection“ verwendet die folgende Syntax:

```
CreateConnection
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConnectionName|-cn> connection_name
[<-ConnectionId|-cid> connection_id]
<-ConnectionType|-ct> connection_type
[<-ConnectionUserName|-cun> connection_user_name]
[<-ConnectionPassword|-cpd> connection_password]
[<-VendorId|-vid> vendor_id]
[-o options] (name-value pairs separated by space)
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateConnection“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ConnectionName -cn	connection_name	Name der Verbindung. Der Name unterliegt nicht der Groß-/ Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die maximale Länge beträgt 128 Zeichen. Das Leer- und die folgenden Sonderzeichen sind möglich: ~ ` ! \$ % ^ & * ( ) - + = { [ } ]   \ : ; " ' < , > . ? /
- ConnectionId -cid	connection_id	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.



Option	Argument	Beschreibung
-ConnectionType -ct	connection_type	<p>Erforderlich. Typ der Verbindung. Verwenden Sie einen der folgenden Verbindungstypen:</p> <ul style="list-style-type: none"> <li>- ADABAS</li> <li>- ADLSGEN1 (Microsoft Azure Data Lake Storage Gen1)</li> <li>- ADLSGEN2 (Microsoft Azure Data Lake Storage Gen2)</li> <li>- AMAZONKINESIS</li> <li>- AMAZONREDSHIFT</li> <li>- AMAZONS3</li> <li>- AZUREBLOB (Microsoft Azure Blob Storage)</li> <li>- BIGQUERY (Google BigQuery)</li> <li>- BLOCKCHAIN</li> <li>- CASSANDRA</li> <li>- ConfluentKafka</li> <li>- DATABRICKS</li> <li>- DATASIFT</li> <li>- DB2</li> <li>- DB2I</li> <li>- DB2Z</li> <li>- FACEBOOK</li> <li>- GreenplumPT</li> <li>- GOOGLLEANALYTICS</li> <li>- GOOGLESTORAGEV2</li> <li>- HADOOP</li> <li>- HBASE</li> <li>- HDFS</li> <li>- HIVE</li> <li>- IBMDB2</li> <li>- IMS</li> <li>- JDBC</li> <li>- JDBC V2</li> <li>- JDEDWARDS ENTERPRISE ONE</li> <li>- KAFKA</li> <li>- LDAP</li> <li>- LINKEDIN</li> <li>- MAPR-DB</li> <li>- Microsoft Azure SQL Data Warehouse</li> <li>- MSDYNAMICS</li> <li>- NETEZZA</li> <li>- ODATA</li> <li>- ODBC</li> <li>- ORACLE</li> <li>- SALESFORCE</li> <li>- SFMC (Salesforce Marketing Cloud)</li> <li>- SAPAPPLICATIONS</li> <li>- SEQ</li> <li>- SFDC</li> <li>- SNOWFLAKE</li> <li>- SPANNERGOOGLE (Google Cloud Spanner)</li> <li>- SQLSERVER</li> <li>- TABLEAU</li> <li>- TABLEAU V3</li> <li>- TERADATA PARALLEL TRANSPORTER</li> <li>- TWITTER</li> <li>- TWITTERSTREAMING</li> <li>- VSAM</li> <li>- WEBCONTENT - KAPOWKATALYST</li> </ul> <p>Sie können den <code>infacmd</code> <code>isp ListConnections</code>-Befehl verwenden, um Verbindungstypen anzuzeigen.</p>

Option	Argument	Beschreibung
ConnectionUserName -cun	connection_us er_name	Erforderlich. Name des Datenbankbenutzers.

Option	Argument	Beschreibung
-ConnectionPassword -cpd	connection_password	<p>Erforderlich. Passwort für den Datenbankbenutzernamen. Sie können ein Passwort mit der Option -cpd oder der Umgebungsvariable INFA_DEFAULT_CONNECTION_PASSWORD festlegen. Wenn Sie das Passwort mit beiden Optionen festlegen, hat das mit der Option -cpd festgelegte Passwort Vorrang.</p> <p>Wenn Sie eine ADABAS-, DB2I-, DB2Z-, IMS-, SEQ- oder VSAM-Verbindung erstellen, können Sie statt eines Passworts eine gültige PowerExchange-Passphrase eingeben. Passphrasen für den Zugriff auf Datenbanken und Datasets auf z/OS können zwischen 9 und 128 Zeichen umfassen. Passphrasen für den Zugriff auf DB2 für i5/OS können maximal 31 Zeichen umfassen. Passphrasen können die folgenden Zeichen enthalten:</p> <ul style="list-style-type: none"> <li>- Groß- und Kleinbuchstaben</li> <li>- Die Zahlen 0 bis 9</li> <li>- Leerzeichen</li> <li>- Die folgenden Sonderzeichen: ' - ; # \ , . / ! % &amp; * ( ) _ + { } : @   &lt; &gt; ?</li> </ul> <p><b>Hinweis:</b> Das erste Zeichen ist ein Apostroph.</p> <p>Passphrasen dürfen keine einfachen Anführungszeichen ('), doppelten Anführungszeichen (") oder Währungssymbole enthalten.</p> <p>Wenn eine Passphrase Leerzeichen enthält, müssen Sie sie in doppelte Anführungszeichen setzen. Beispiel: „Das ist eine Beispiel-Passphrase“. Wenn eine Passphrase Sonderzeichen enthält, müssen Sie sie in dreifache doppelte Anführungszeichen (""") setzen. Beispiel: """"Diese Passphrase enthält Sonderzeichen. % &amp; *. """".</p> <p>Wenn eine Passphrase nur alphanumerische Zeichen ohne Leerzeichen enthält, können Sie sie ohne Delimiter eingeben.</p> <p><b>Hinweis:</b> Auf z/OS kann eine gültige RACF-Passphrase bis zu 100 Zeichen umfassen. PowerExchange schneidet Passphrases mit mehr als 100 Zeichen ab, wenn diese zur Validierung an RACF übergeben werden.</p> <p>Stellen Sie vor der Verwendung von Passphrasen sicher, dass der PowerExchange-Listenerdienst im DBMOVER-Mitglied mit der Sicherheitseinstellung SECURITY=(1,N) oder höher ausgeführt wird. Weitere Informationen finden Sie unter „SECURITY-Anweisung“ im <i>PowerExchange-Referenzhandbuch</i>.</p> <p>Stellen Sie zur Verwendung von Passphrasen für IMS-Verbindungen sicher, dass die folgenden zusätzlichen Anforderungen erfüllt sind:</p> <ul style="list-style-type: none"> <li>- Sie müssen ODBA-Zugriff auf IMS wie im <i>PowerExchange-Navigator-Benutzerhandbuch</i> erläutert konfigurieren.</li> <li>- Sie müssen IMS-Daten-Mappings verwenden, die IMS ODBA als Zugriffsmethode angeben. Verwenden Sie keine Daten-Mappings, die die DL/1 BATCH-Zugriffsmethode angeben, da diese Zugriffsmethode die Verwendung von Netport-Jobs erfordert, die keine Unterstützung für Passphrases bieten.</li> <li>- Die IMS-Datenbank muss im IMS-Kontrollbereich online sein, um ODBA-Zugriff auf IMS zu verwenden.</li> </ul>

Option	Argument	Beschreibung
-VendorId -vid	vendor_id	Optional. ID des externen Partners, der den Adapter erstellt hat.
-Options -o	options	Erforderlich. Geben Sie Name-Wert-Paare durch Leerzeichen getrennt ein. Die Verbindungsoptionen sind für jeden Verbindungstyp unterschiedlich.  Verwenden Sie einfache Anführungszeichen, um ein beliebiges Gleichheits- oder Leerzeichen im Wert zu vermeiden.

## Adabas-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Adabas-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

- Trennen Sie mehrere Optionen mit einem Leerzeichen.
- Schließen Sie Parameter, die ein Gleichheitszeichen (=) enthalten, in einfache Anführungszeichen ein.

```
... -o option_name=value option_name=value ...
```

In der folgenden Tabelle werden die Adabas-Verbindungsoptionen beschrieben:

Option	Beschreibung
CodePage	Erforderlich. Code zum Lesen aus oder Schreiben in die Datenbank. Verwenden Sie den ISO-Codepage-Namen, z. B. ISO-8859-6. Der Codepage-Name berücksichtigt keine Groß- und Kleinschreibung.
ArraySize	Optional. Bestimmt die Anzahl der Datensätze im Speicher-Array für die Threads, wenn der Worker-Threads-Wert größer als 0 ist. Gültige Werte sind 1 bis 5000. Standardwert ist 25.
Komprimierung	Optional. Komprimiert die Daten, um die Menge an Daten zu reduzieren, die Informatica-Anwendungen über das Netzwerk schreiben. „True“ oder „False“. Standardwert ist „False“.
EncryptionLevel	Optional. Verschlüsselungsebene. Wenn Sie AES für die Option EncryptionType angeben, müssen Sie einen der folgenden Werte angeben, um die Ebene der AES-Verschlüsselung anzugeben: <ul style="list-style-type: none"> <li>- 1. Verwenden Sie einen 128-Bit-Verschlüsselungsschlüssel.</li> <li>- 2. Verwenden Sie einen 192-Bit-Verschlüsselungsschlüssel.</li> <li>- 3. Verwenden Sie einen 256-Bit-Verschlüsselungsschlüssel.</li> </ul> Standardwert ist 1. <b>Hinweis:</b> Wenn Sie für den Verschlüsselungstyp „Keine“ auswählen, ignoriert der Datenintegrationsdienst den Wert für die Verschlüsselungsebene.
EncryptionType	Optional. Steuert, ob Verschlüsselung verwendet werden soll. Geben Sie einen der folgenden Werte an: <ul style="list-style-type: none"> <li>- Keine</li> <li>- AES</li> </ul> Standardwert ist „Keine“.
InterpretAsRows	Optional. Bei TRUE gibt die Pacing-Größe eine Anzahl von Zeilen wieder. Bei „false“ gibt die Pacing-Größe Kilobyte wieder. Standardwert ist „false“.

Option	Beschreibung
Speicherort:	Speicherort des PowerExchange Listener-Knotens, der eine Verbindung zur Datenbank herstellen kann. Der Speicherort ist im ersten Parameter der NODE-Anweisung in der PowerExchange-Konfigurationsdatei „dbmover.cfg“ angegeben.
OffLoadProcessing	Optional. Verschiebt die Stapeldatenverarbeitung vom Quellcomputer zum Computer des Datenintegrationsdiensts. Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- Auto. Der Datenintegrationsdienst bestimmt, ob Offload-Verarbeitung verwendet werden soll.</li> <li>- Ja. Offload-Verarbeitung wird verwendet.</li> <li>- Nein. Offload-Verarbeitung wird nicht verwendet.</li> </ul> Standardwert ist „Auto“.
PacingSize	Optional. Verlangsamt die Datenübertragungsrate, um Engpässe zu reduzieren. Je geringer der Wert ist, desto höher ist die Sitzungsleistung. Der Mindestwert lautet 0. Geben Sie 0 für optimale Leistung ein. Standardwert ist 0.
WorkerThread	Optional. Anzahl der vom Datenintegrationsdienst verwendeten Threads, um Stapeldaten bei aktivierter Offload-Verarbeitung zu verarbeiten. Um eine optimale Leistung zu erzielen, sollte dieser Wert die Anzahl der verfügbaren Prozessoren auf dem Rechner des Datenintegrationsdienstes nicht überschreiten. Gültige Werte sind 1 bis 64. Standardwert ist 0, wodurch Multithreading deaktiviert wird.
WriteMode	Geben Sie einen der folgenden Schreibmodi ein: <ul style="list-style-type: none"> <li>- CONFIRMWRITEON. Sendet Daten zum PowerExchange Listener und wartet auf eine Erfolgs-/Nichterfolgsreaktion, bevor weitere Daten gesendet werden.</li> <li>- CONFIRMWRITEOFF. Sendet Daten zum PowerExchange Listener, ohne eine Erfolgs-/Nichterfolgsreaktion abzuwarten. Verwenden Sie diese Option, wenn die Target-Tabelle bei Auftreten eines Fehlers erneut geladen werden kann.</li> <li>- ASYNCHRONOUSWITHFAULTT. Sendet Daten asynchron zum PowerExchange Listener mit der Möglichkeit der Fehlererkennung.</li> </ul> Der Standardwert ist CONFIRMWRITEON.
EnableConnectionPool	Optional. Aktiviert das Verbindungspooling. Wenn Sie Verbindungspooling aktivieren, behält der Verbindungspool inaktive Verbindungsinstanzen im Speicher. Wenn Sie Verbindungspooling deaktivieren, stoppt der Datenintegrationsdienst alle Poolingaktivitäten. „True“ oder „False“. Standardwert ist „False“.
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Datenintegrationsdienst für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Standardwert ist 15.
ConnectionPoolMaxIdleTime	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird. Standardwert ist 120.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Standardwert ist 0.

## Amazon Kinesis-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Amazon Kinesis-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Führen Sie beispielsweise folgenden Befehl aus, um mithilfe der kontenübergreifenden IAM-Rolle eine Amazon Kinesis-Verbindung mit Kinesis Streams unter UNIX zu erstellen:

```
infacmd createConnection -dn <domain name> -un <domain user> -pd <domain password> -cn  
<connection name> -cid <connection id> -ct AMAZONKINESIS -o "AWS_ACCESS_KEY_ID=<access  
key id> AWS_SECRET_ACCESS_KEY=<secret access key> ConnectionTimeout=10000  
Region=<RegionName> ServiceType='Kinesis Streams' RoleArn=<ARN of IAM role>  
ExternalID=<External ID> AuthenticationType='Cross-account IAM Role'"
```

Führen Sie folgenden Befehl aus, um mithilfe des AWS-Anmeldedatenprofils eine Amazon Kinesis-Verbindung mit Kinesis Firehose unter UNIX zu erstellen:

```
infacmd createConnection -dn <domain name> -un <domain user> -pd <domain password> -cn  
<connection name> -cid <connection id> -ct AMAZONKINESIS -o "AWS_ACCESS_KEY_ID=<access  
key id> AWS_SECRET_ACCESS_KEY=<secret access key> ConnectionTimeout=10000  
Region=<RegionName> ServiceType='Kinesis Firehose' Profilename=<AWS credential profile>  
AuthenticationType='AWS Credential Profile'"
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden Amazon Kinesis-Verbindungsoptionen für den Befehl „infacmd isp CreateConnection“ beschrieben:

Eigenschaft	Beschreibung
AWS_ACCESS_KEY_ID	Die Zugriffsschlüssel-ID für das Amazon AWS-Benutzerkonto.
AWS_SECRET_ACCESS_KEY	Der geheime Zugriffsschlüssel für das Amazon AWS-Benutzerkonto.
ConnectionTimeout	Anzahl der Millisekunden, die der Integrationsdienst bis zum Herstellen einer Verbindung mit Kinesis Stream oder Kinesis Firehose wartet, bevor eine Zeitüberschreitung eintritt.
Region	Region, in der der Endpunkt für den Dienst verfügbar ist. Dafür können Sie einen der folgenden Werte auswählen: <ul style="list-style-type: none"><li>- us-east-2. Gibt die Region US East (Ohio) an.</li><li>- us-east-1. Gibt die Region US East (Nord-Virginia) an.</li><li>- us-west-1. Gibt die Region US West (Nordkalifornien) an.</li><li>- us-west-2. Gibt die Region US West (Oregon) an.</li><li>- ap-northeast-1. Gibt die Region Asien-Pazifik (Tokio) an.</li><li>- ap-northeast-2. Gibt die Region Asien-Pazifik (Seoul) an.</li><li>- ap-northeast-3. Gibt die Region Asien-Pazifik (Osaka-Lokal) an.</li><li>- ap-south-1. Gibt die Region Asien-Pazifik (Mumbai) an.</li><li>- ap-southeast-1. Gibt die Region Asien-Pazifik (Singapur) an.</li><li>- ap-southeast-2. Gibt die Region Asien-Pazifik (Sidney) an.</li><li>- ca-central-1. Gibt die Region Kanada (Central) an.</li><li>- cn-north-1. Gibt die Region China (Peking) an.</li><li>- cn-northwest-1. Gibt die Region China (Ningxia) an.</li><li>- eu-central-1. Gibt die Region EU (Frankfurt) an.</li><li>- eu-west-1. Gibt die Region EU (Irland) an.</li><li>- eu-west-2. Gibt die Region EU (London) an.</li><li>- eu-west-3. Gibt die Region EU (Paris) an.</li><li>- sa-east-1. Gibt die Region Südamerika (São Paulo) an.</li></ul>

Eigenschaft	Beschreibung
ServiceType	Der Typ des Kinesis-Diensts, dem die Verbindung zugeordnet ist. Wählen Sie einen der folgenden Diensttypen aus: <ul style="list-style-type: none"> <li>- Kinesis Firehose. Wählen Sie diesen Dienst zum Schreiben in Kinesis Firehose Delivery Stream aus.</li> <li>- Kinesis Streams. Wählen Sie diesen Dienst zum Lesen aus Kinesis Streams aus.</li> </ul>
Profilname	Erforderlich, wenn Sie den Authentifizierungstyp „AWS-Anmeldedatenprofil“ verwenden. Ein in der Anmeldedatendatei definiertes AWS-Anmeldedatenprofil. Eine Zuordnung greift zur Laufzeit über den Profilnamen auf die AWS-Anmeldedaten zu. Wenn Sie keinen Namen für das AWS-Anmeldedatenprofil bereitstellen, verwendet die Zuordnung die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel, die Sie beim Erstellen der Verbindung angegeben haben.
RoleArn	Erforderlich, wenn Sie den Authentifizierungstyp „Kontenübergreifende IAM-Rolle“ verwenden. Der Name der Amazon-Ressource zur Angabe der Rolle eines IAM-Benutzers.
ExternalID	Erforderlich, wenn Sie den Authentifizierungstyp „Kontenübergreifende IAM-Rolle“ verwenden und die externe ID vom AWS-Konto definiert wird. Bei der externen ID für eine IAM-Rolle handelt es sich um eine zusätzliche Einschränkung, die Sie in einer Vertrauensrichtlinie der IAM-Rolle zum Festlegen des Benutzers verwenden können, der die IAM-Rolle übernehmen soll.
AuthenticationType	Der Authentifizierungstyp. Wählen Sie einen der folgenden Werte aus: <ul style="list-style-type: none"> <li>- AWS-Anmeldedatenprofil</li> <li>- Kontenübergreifende IAM-Rolle</li> </ul> Der Standardwert lautet „AWS-Anmeldedatenprofil“.

## Verbindungsoptionen für Amazon Redshift

Verwenden Sie Verbindungsoptionen zum Definieren einer Amazon Redshift-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die obligatorischen Verbindungsoptionen für Amazon Redshift für die Befehle `infacmd` und `isp` `CreateConnection` und `UpdateConnection` beschrieben:

Eigenschaft	Beschreibung
Benutzername	Benutzername des Amazon Redshift-Kontos.
Passwort	Passwort für das Amazon Redshift-Konto.
Zugriffsschlüssel-ID	Zugriffsschlüssel-ID für Amazon S3-Bucket. <b>Hinweis:</b> Erforderlich, wenn Sie nicht die IAM-Authentifizierung (AWS Identity and Access Management) verwenden.

Eigenschaft	Beschreibung
Geheimer Zugriffsschlüssel	ID des geheimen Zugriffsschlüssels für Amazon S3-Bucket. <b>Hinweis:</b> Erforderlich, wenn Sie nicht die IAM-Authentifizierung (AWS Identity and Access Management) verwenden.
Symmetrischer Hauptschlüssel	Optional. Stellen Sie bei der Aktivierung der clientseitigen Verschlüsselung einen 256-Bit-AES-Verschlüsselungsschlüssel im Base64-Format bereit. Sie können einen Schlüssel mit einem Drittanbieter-Tool generieren.  Wenn Sie einen Wert angeben, stellen Sie sicher, dass Sie den Verschlüsselungstyp in den erweiterten Zieleigenschaften als clientseitige Verschlüsselung angeben.
JDBC-URL	Verbindungs-URL für Amazon Redshift.



Eigenschaft	Beschreibung
Clusterregion	<p>Optional. Die AWS-Clusterregion, in der sich der Bucket befindet, auf den Sie zugreifen möchten.</p> <p>Wählen Sie eine Clusterregion aus, wenn Sie eine benutzerdefinierte JDBC-URL bereitstellen möchten, die keinen Clusterregionsnamen in der Verbindungseigenschaft <b>JDBC-URL</b> enthält.</p> <p>Wenn Sie eine Clusterregion in den Verbindungseigenschaften <b>Clusterregion</b> und <b>JDBC-URL</b> angeben, ignoriert der Datenintegrationsdienst die Clusterregion, die Sie in der Verbindungseigenschaft <b>JDBC-URL</b> festgelegt haben.</p> <p>Zur Verwendung des Clusterregionsnamens, den Sie in der Verbindungseigenschaft <b>JDBC-URL</b> angegeben haben, wählen Sie <b>Keine</b> als Clusterregion in dieser Eigenschaft aus.</p> <p>Wählen Sie eine der folgenden Clusterregionen aus:</p> <p>Wählen Sie eine der folgenden Regionen aus:</p> <ul style="list-style-type: none"> <li>- Asien-Pazifik (Mumbai)</li> <li>- Asien-Pazifik (Seoul)</li> <li>- Asien-Pazifik (Singapur)</li> <li>- Asien-Pazifik (Sydney)</li> <li>- Asien-Pazifik (Tokio)</li> <li>- AWS GovCloud (USA)</li> <li>- Kanada (Zentral)</li> <li>- China (Peking)</li> <li>- China (Ningxia)</li> <li>- EU (Irland)</li> <li>- EU (Frankfurt)</li> <li>- EU (London)</li> <li>- EU (Paris)</li> <li>- Südamerika (São Paulo)</li> <li>- USA, Osten (Ohio)</li> <li>- USA, Osten (Northern Virginia)</li> <li>- USA, Westen (Nordkalifornien)</li> <li>- USA, Westen (Oregon)</li> </ul> <p>Standardwert ist „Kein“.</p> <p>Daten können nur in die Clusterregionen geschrieben oder aus den Clusterregionen gelesen werden, die von dem AWS-SDK unterstützt werden, das von PowerExchange for Amazon Redshift verwendet wird.</p>
Kunden-Master-Schlüssel-ID	<p>Optional. Geben Sie die ID des Kunden-Master-Schlüssels an, der von AWS Key Management Service (AWS KMS) oder dem Amazon Resource Name (ARN) Ihres benutzerdefinierten Schlüssels für kontoübergreifenden Zugriff verwendet wird. Sie müssen den Kunden-Master-Schlüssel entsprechend der Region erzeugen, in der sich das Amazon S3-Bucket befindet. Sie können einen der folgenden Werte angeben:</p> <p><b>Vom Kunden erzeugter Kunden-Master-Schlüssel</b></p> <p>Aktiviert client- oder serverseitige Verschlüsselung.</p> <p><b>Standardmäßiger Kunden-Master-Schlüssel</b></p> <p>Aktiviert client- oder serverseitige Verschlüsselung. Nur der Administratorbenutzer des Kontos kann die standardmäßige Kunden-Master-Schlüssel-ID verwenden, um clientseitige Verschlüsselung zu aktivieren.</p>

## Verbindungsoptionen für Amazon S3

Verwenden Sie Verbindungsoptionen zum Definieren einer Amazon S3-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die obligatorischen Verbindungsoptionen für Amazon S3 für die Befehle `infacmd isp CreateConnection` und `UpdateConnection` beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * ( ) - + = { [ ] }   \ : ; ' " < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Optional. Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Amazon S3-Verbindungstyp.
Zugriffsschlüssel	Zugriffsschlüssel für den Zugriff auf den Amazon S3-Bucket. Stellen Sie den Wert des Zugriffsschlüssels anhand der folgenden Authentifizierungsmethoden bereit: <ul style="list-style-type: none"> <li>- Standardauthentifizierung: Bereitstellung des tatsächlichen Zugriffsschlüsselwerts.</li> <li>- IAM-Authentifizierung: Keine Bereitstellung des Zugriffsschlüsselwerts.</li> <li>- Temporäre Sicherheitsanmeldedaten mittels der übernommenen Rolle: Bereitstellung des Zugriffsschlüssels eines IAM-Benutzers ohne Berechtigung zum Zugriff auf den Amazon S3-Bucket.</li> </ul>
Geheimer Schlüssel	Geheimer Schlüssel für den Zugriff auf den Amazon S3-Bucket. Der geheime Schlüssel ist mit dem Zugriffsschlüssel verknüpft und identifiziert das Konto eindeutig. Stellen Sie den Wert des Zugriffsschlüssels anhand der folgenden Authentifizierungsmethoden bereit: <ul style="list-style-type: none"> <li>- Standardauthentifizierung: Bereitstellung des tatsächlichen Werts des Zugriffsgeheimworts.</li> <li>- IAM-Authentifizierung: Keine Bereitstellung des Werts des Zugriffsgeheimworts.</li> <li>- Temporäre Sicherheitsanmeldedaten mittels der übernommenen Rolle: Bereitstellung des Zugriffsgeheimworts eines IAM-Benutzers ohne Berechtigung zum Zugriff auf den Amazon S3-Bucket.</li> </ul>
ARN der IAM-Rolle	Der ARN der IAM-Rolle, die der Benutzer annimmt, um die dynamisch generierten temporären Sicherheitsanmeldedaten zu verwenden. Geben Sie den Wert dieser Eigenschaft ein, wenn Sie die temporären Sicherheitsanmeldedaten für den Zugriff auf die AWS-Ressourcen verwenden möchten. Wenn Sie die temporären Sicherheitsanmeldedaten mit IAM-Authentifizierung verwenden möchten, geben Sie die Verbindungseigenschaften „Zugriffsschlüssel“ und „Geheimer Schlüssel“ nicht an. Wenn Sie die temporären Sicherheitsanmeldedaten ohne IAM-Authentifizierung verwenden möchten, müssen Sie den Wert der Verbindungseigenschaften „Zugriffsschlüssel“ und „Geheimer Schlüssel“ eingeben. Weitere Informationen darüber, wie Sie den ARN der IAM-Rolle erhalten, finden Sie in der AWS-Dokumentation.

Eigenschaft	Beschreibung
Ordnerpfad	<p>Der vollständige Pfad zu Amazon S3-Objekten. Der Pfad muss den Bucket-Namen und alle Ordernamen einschließen.</p> <p>Verwenden Sie keinen Schrägstrich am Ende des Ordnerpfads. Beispiel: &lt;Bucket-Name&gt;/&lt;Name meines Ordners&gt;.</p>
Symmetrischer Hauptschlüssel	<p>Optional. Stellen Sie bei der Aktivierung der clientseitigen Verschlüsselung einen 256-Bit-AES-Verschlüsselungsschlüssel im Base64-Format bereit. Sie können mit einem Drittanbieter-Tool einen symmetrischen Hauptschlüssel generieren.</p>
S3-Kontotyp	<p>Der Typ des Amazon S3-Kontos.</p> <p>Wählen Sie <b>Amazon S3-Speicher</b> oder <b>S3-kompatibler Speicher</b> aus.</p> <p>Wählen Sie die Amazon S3-Speicheroption aus, um die Amazon S3-Dienste zu nutzen. Wählen Sie die S3-kompatible Speicheroption aus, um den Endpunkt für einen externen Speicheranbieter wie Scality RING anzugeben.</p> <p>Standardmäßig ist Amazon S3-Speicher ausgewählt.</p>
REST-Endpunkt	<p>Der S3-Speicherendpunkt.</p> <p>Geben Sie den S3-Speicherendpunkt im HTTP/HTTPS-Format an, wenn Sie die Option für den S3-kompatiblen Speicher auswählen. Beispiel: <a href="http://s3.isv.scality.com">http://s3.isv.scality.com</a>.</p>
Name der Region	<p>Wählen Sie die AWS-Region, in der sich der Bucket befindet, auf den Sie zugreifen möchten.</p> <p>Wählen Sie eine der folgenden Regionen aus:</p> <ul style="list-style-type: none"> <li>- Asien-Pazifik (Mumbai)</li> <li>- Asien-Pazifik (Seoul)</li> <li>- Asien-Pazifik (Singapur)</li> <li>- Asien-Pazifik (Sydney)</li> <li>- Asien-Pazifik (Tokio)</li> <li>- AWS GovCloud (USA)</li> <li>- Kanada (Zentral)</li> <li>- China (Peking)</li> <li>- China (Hongkong)</li> <li>- China (Ningxia)</li> <li>- EU (Irland)</li> <li>- EU (Frankfurt)</li> <li>- EU (London)</li> <li>- EU (Paris)</li> <li>- Südamerika (São Paulo)</li> <li>- USA, Osten (Ohio)</li> <li>- USA, Osten (Northern Virginia)</li> <li>- USA, Westen (Nordkalifornien)</li> <li>- USA, Westen (Oregon)</li> </ul> <p>Der Standardwert ist Östliche USA (N. Virginia).</p> <p>Gilt nicht für S3-kompatiblen Speicher.</p>

Eigenschaft	Beschreibung
Kunden-Master-Schlüssel-ID	<p>Optional. Geben Sie die ID des Kunden-Master-Schlüssels oder den Aliasnamen an, der von AWS Key Management Service (AWS KMS) oder dem Amazon Resource Name (ARN) Ihres benutzerdefinierten Schlüssels für kontoübergreifenden Zugriff verwendet wird. Sie müssen den Kunden-Master-Schlüssel für dieselbe Region erzeugen, in der sich das Amazon S3-Bucket befindet.</p> <p>Sie können einen der folgenden Werte angeben:</p> <p><b>Vom Kunden erzeugter Kunden-Master-Schlüssel</b></p> <p>Aktiviert client- oder serverseitige Verschlüsselung.</p> <p><b>Standardmäßiger Kunden-Master-Schlüssel</b></p> <p>Aktiviert client- oder serverseitige Verschlüsselung. Nur der Administratorbenutzer des Kontos kann die standardmäßige Kunden-Master-Schlüssel-ID verwenden, um clientseitige Verschlüsselung zu aktivieren.</p>
Verbund-SSO-IdP	<p>SAML 2.0-fähiger Identitätsanbieter für ein Single Sign-On von föderierten Benutzern zur Verwendung mit dem AWS-Konto.</p> <p>PowerExchange for Amazon S3 unterstützt nur den Identitätsanbieter ADFS 3.0.</p> <p>Wählen Sie <code>Kein</code>, wenn Sie kein Single Sign-On für föderierte Benutzer verwenden möchten.</p>

## Verbindungseigenschaften für Single Sign-On für föderierte Benutzer

Konfigurieren Sie die folgenden Eigenschaften, wenn Sie ADFS 3.0 in **Föderierter SSO-IdP** auswählen:

Eigenschaft	Beschreibung
Name des föderierten Benutzers	Benutzername des föderierten Benutzers für den Zugriff auf das AWS-Konto über den Identitätsanbieter.
Passwort des föderierten Benutzers	Passwort des föderierten Benutzers für den Zugriff auf das AWS-Konto über den Identitätsanbieter.
IdP-SSO-URL	Single Sign-On-URL des Identitätsanbieters für AWS.
SAML-Identitätsanbieter-ARN	ARN des SAML-Identitätsanbieters, die der AWS-Administrator erstellt hat, um den Identitätsanbieter als vertrauenswürdigen Anbieter zu registrieren.
Rollen-ARN	ARN der vom föderierten Benutzer angenommenen IAM-Rolle.

## Blockchain-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Blockchain-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alfanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Blockchain-Verbindungsoptionen für die Befehle „infacmd isp CreateConnection“ und „infacmd isp UpdateConnection“ beschrieben:

Eigenschaft	Beschreibung
swaggerFilePath	Der absolute Pfad des Swagger-Dateipfades, der die REST-API für die Kommunikation mit der Blockchain enthält. Die Swagger-Datei muss eine JSON-Datei sein, die auf dem Computer mit dem Datenintegrationsdienst gespeichert ist. Falls die Swagger-Datei in einem anderen Dateiformat wie beispielsweise YAML vorliegt, konvertieren Sie die Daten in das JSON-Format.
authType*	Authentifizierungsmethode, mit dem sich die Laufzeit-Engine mit dem REST-Server verbindet. Sie können „none“, „basic“, „digest“ oder „OAuth“ verwenden.
authUserID*	Benutzername zur Authentifizierung beim REST-Server.
authPassword*	Passwort für den Benutzernamen zur Authentifizierung beim REST-Server.
oAuthConsumerKey*	Für den OAuth-Authentifizierungstyp erforderlich. Clientschlüssel, der dem REST-Server zugeordnet ist.
oAuthConsumerSecret*	Für den OAuth-Authentifizierungstyp erforderlich. Clientpasswort für die Verbindung zum REST-Server.
oAuthToken*	Für den OAuth-Authentifizierungstyp erforderlich. Zugriffstoken für die Verbindung zum REST-Server.
oAuthTokenSecret*	Für den OAuth-Authentifizierungstyp erforderlich. Passwort, das dem OAuth-Token zugeordnet ist.
proxyType*	Typ des Proxy. Sie können „no proxy“, „platform proxy“ oder „custom“ verwenden.
proxyDetails*	Proxy-Konfiguration mit dem Format <host>:<port>.
trustStoreFilePath*	Der absolute Pfad für die Truststore-Datei, die das SSL-Zertifikat enthält.
trustStorePassword*	Passwort für die TrustStore-Datei
keyStoreFilePath*	Der absolute Pfad der Schlüsselspeicherdatei, die die Schlüssel und Zertifikate enthält, die zum Herstellen einer sicheren Zwei-Wege-Verbindung mit dem REST-Server benötigt werden.
keyStorePassword*	Passwort für die Schlüsselspeicherdatei
advancedProperties	<p>Liste der erweiterten Eigenschaften für den Zugriff auf ein Objekt in der Blockchain. Geben Sie die erweiterten Eigenschaften anhand von Name/Wert-Paaren an, die durch ein Semikolon getrennt sind.</p> <p>Sie können die folgenden erweiterten Eigenschaften verwenden:</p> <ul style="list-style-type: none"> <li>- BaseUrl. Erforderlich, wenn die Swagger-Datei nicht die Basis-URL enthält. Die Basis-URL, die für den Zugriff auf Objekte in der Blockchain verwendet wird.</li> <li>- X-API-KEY. Erforderlich, wenn Sie sich mithilfe eines API-Schlüssels beim REST-Server authentifizieren.</li> </ul> <p>Die erweiterten Eigenschaften, die Sie in der Verbindung konfigurieren, überschreiben die Werte für die entsprechenden erweiterten Eigenschaften im Blockchain-Datenobjekt. Wenn beispielsweise sowohl die Verbindung als auch das Datenobjekt beide eine Basis-URL, überschreibt der Wert in der Verbindung den Wert im Datenobjekt.</p>

Eigenschaft	Beschreibung
Cookies	<p>Erforderlich, je nachdem, wie die REST-API implementiert ist. Liste der Cookie-Eigenschaften, um die Cookie-Informationen anzugeben, die an den REST-Server übergeben werden. Geben Sie die Eigenschaften anhand von Name/Wert-Paaren an, die durch ein Semikolon getrennt sind.</p> <p>Die Cookie-Eigenschaften, die Sie in der Verbindung konfigurieren, überschreiben die Werte für die entsprechenden Cookie-Eigenschaften im Blockchain-Datenobjekt.</p>
<p>* Die Eigenschaft wird ignoriert. Um die Funktionalität zu nutzen, konfigurieren Sie die Eigenschaft als erweiterte Eigenschaft und stellen Sie ein Name/Wert-Paar bereit, das auf dem Eigenschaftsnamen in der Swagger-Datei basiert. Konfigurieren Sie z. B. das folgende Name/Wert-Paar zur Verwendung der grundlegenden Autorisierung:</p> <p>Authorization=Basic &lt;credentials&gt;</p>	

## Cassandra-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren der Cassandra-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Beispiel:

```
./infacmd.sh createConnection -dn Domain Adapters_1020_Uni -un Administrator -pd
Administrator -cn Cassandra_test2 -ct CASSANDRA -cun cloud2 -cpd cloud2 -o
HostName=invrlx7acdb01 DefaultKeyspace=cloud SQLIDENTIFIERCHARACTER='"'(quotes) '
SSLMODE=disabled
AdditionalConnectionProperties='BinaryColumnLength=10000;DecimalColumnScale=19;EnableCaseS
ensitive=0;EnableNullInsert=1;EnablePaging=0;
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Cassandra-Verbindungsoptionen für die Befehle „infacmd isp CreateConnection“ und „infacmd isp UpdateConnection“ beschrieben:

Eigenschaft	Beschreibung
HostName	Hostname oder IP-Adresse des Cassandra-Servers.
Port	Portnummer des Cassandra-Servers. Standardwert ist 9042.
User Name -cun	Benutzername für den Zugriff auf den Cassandra-Server.
Password -cpd	Zum Benutzernamen gehöriges Passwort für den Zugriff auf den Cassandra-Server.
DefaultKeyspace	Name des standardmäßig zu verwendenden Cassandra-Schlüsselspeichers.

Eigenschaft	Beschreibung
SQLIDENTIFIERCHARACTER	<p>Typ des Zeichens, das von der Datenbank verwendet wird, um Delimiterbezeichner in SQL- oder CQL-Abfragen einzuschließen. Welche Zeichen verfügbar sind, richtet sich nach dem Datenbanktyp.</p> <p>Geben Sie <b>Keine</b> an, wenn die Datenbank reguläre Bezeichner verwendet. Wenn der Datenintegrationsdienst SQL- oder CQL-Abfragen erzeugt, werden die Bezeichner nicht in Delimitern eingeschlossen.</p> <p>Geben Sie ein Zeichen an, wenn die Datenbank Delimiterbezeichner verwendet. Wenn der Datenintegrationsdienst SQL- oder CQL-Abfragen erzeugt, schließt der Dienst Delimiterbezeichner in dieses Zeichen ein.</p>
SSLMODE	<p>Für PowerExchange for Cassandra JDBC nicht anwendbar.</p> <p>Geben Sie <b>deaktiviert</b> ein.</p>
AdditionalConnectionProperties	<p>Geben Sie einen oder mehrere JDBC-Verbindungsparameter in folgendem Format ein:</p> <p>&lt;param1&gt;=&lt;value&gt;;&lt;param2&gt;=&lt;value&gt;;&lt;param3&gt;=&lt;value&gt;</p> <p>PowerExchange for Cassandra JDBC unterstützt die folgenden JDBC-Verbindungsparameter:</p> <ul style="list-style-type: none"> <li>- BinaryColumnLength</li> <li>- DecimalColumnScale</li> <li>- EnableCaseSensitive</li> <li>- EnableNullInsert</li> <li>- EnablePaging</li> <li>- RowsPerPage</li> <li>- StringColumnLength</li> <li>- VTTableNameSeparator</li> </ul>

## Confluent Kafka-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Confluent Kafka-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Führen Sie beispielsweise den folgenden Befehl aus, um eine Confluent Kafka-Verbindung unter UNIX zu erstellen:

```
sh infacmd.sh createConnection -dn <domain name> -un <domain user> -pd <domain password>
-cn <connection name> -cid <connection id> -ct ConfluentKafka -o
"kfkBrkList='<host1:port1>,<host2:port2>,<host3:port3>' kafkabrokerverversion='<version>'
schemaregistryurl='<schema registry URL>'"
```

## Databricks-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Databricks-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Databricks-Verbindungsoptionen für die Befehle „`infacmd isp CreateConnection`“ und „`infacmd isp UpdateConnection`“ beschrieben:

Option	Beschreibung
<code>connectionId</code>	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
<code>connectionType</code>	Erforderlich. Verbindungstyp lautet „Databricks“.
<code>name</code>	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/ Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * ( ) - + = { [ ] }   \ : ; " ' < , > . ? /
<code>databricksExecutionParameterList</code>	Erweiterte Eigenschaften, die eigens für die Databricks Spark-Engine gelten. Zur Eingabe mehrerer Eigenschaften trennen Sie jedes Name-Wert-Paar durch folgenden Text: <code>&amp;:.</code> Erweiterte Informatica-Eigenschaften dürfen nur nach Absprache mit dem globalen Kundensupport von Informatica verwendet werden.
<code>clusterConfigId</code>	Name der Cluster-Konfiguration, die mit der Databricks-Umgebung verknüpft ist. Erforderlich, wenn Sie die Cloud-Bereitstellung nicht konfigurieren.
<code>provisionConnectionId</code>	Name der Cloud-Bereitstellungskonfiguration, die einer Cloud-Plattform zugeordnet ist, wie z. B. Microsoft Azure. Erforderlich, wenn Sie den Cluster nicht konfigurieren.
<code>stagingDirectory</code>	Das Verzeichnis, in dem die Databricks Spark-Engine Laufzeitdateien bereitstellt. Wenn Sie ein Verzeichnis angeben, das nicht vorhanden ist, wird es vom Datenintegrationsdienst zur Laufzeit erstellt. Wenn Sie keinen Verzeichnispfad bereitstellen, werden die Staging-Dateien zur Laufzeit in das Verzeichnis <code>/&lt;cluster staging directory&gt;/DATABRICKS</code> geschrieben.

## DataSift-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer DataSift-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.



In der folgenden Tabelle werden die DataSift-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
userName	DataSift-Benutzernamen für das DataSift-Benutzerkonto.
apiKey	API-Schlüssel. Der Developer-API-Schlüssel wird auf dem Dashboard oder auf der Einstellungsseite im DataSift-Benutzerkonto angezeigt.

## DB2 für i5/OS-Verbindungsoptionen

Verwenden Sie DB2I-Verbindungsoptionen, um die DB2 für i5/OS-Verbindung zu definieren.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die DB2 für i5/OS-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
DatabaseName	Datenbankinstanzname.
EnvironmentSQL	Optional. SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt. <b>Hinweis:</b> Setzen Sie Sonderzeichen in doppelte Anführungszeichen.
CodePage	Erforderlich. Codepage, die zum Lesen aus einer Quelldatenbank oder zum Schreiben in eine Zieldatenbank oder -Datei verwendet wird.
ArraySize	Optional. Bestimmt die Anzahl der Datensätze im Speicher-Array für die Threads, wenn der Worker-Threads-Wert größer als 0 ist. Gültige Werte sind 1 bis 5000. Standardwert ist 25.
Komprimierung	Optional. Komprimiert die Daten, um die Menge an Daten zu reduzieren, die über das Netzwerk geschrieben werden. Standardwert ist „false“.
EncryptionLevel	Optional. Verschlüsselungsebene. Wenn Sie AES für die Option EncryptionType angeben, müssen Sie einen der folgenden Werte angeben, um die Ebene der AES-Verschlüsselung anzugeben: <ul style="list-style-type: none"> <li>- 1. Verwenden Sie einen 128-Bit-Verschlüsselungsschlüssel.</li> <li>- 2. Verwenden Sie einen 192-Bit-Verschlüsselungsschlüssel.</li> <li>- 3. Verwenden Sie einen 256-Bit-Verschlüsselungsschlüssel.</li> </ul> Standardwert ist 1. <b>Hinweis:</b> Wenn Sie für den Verschlüsselungstyp „Keine“ auswählen, ignoriert der Datenintegrationsdienst den Wert für die Verschlüsselungsebene.
EncryptionType	Optional. Steuert, ob Verschlüsselung verwendet werden soll. Geben Sie einen der folgenden Werte an: <ul style="list-style-type: none"> <li>- Keine</li> <li>- AES</li> </ul> Standardwert ist „Keine“.

Option	Beschreibung
InterpretAsRows	Optional. Repräsentiert die Pacing-Größe als Anzahl von Zeilen. Bei „false“ gibt die Pacing-Größe Kilobyte wieder. Standardwert ist „false“.
Speicherort:	Speicherort des PowerExchange Listener-Knotens, der eine Verbindung zur Datenbank herstellen kann. Der Speicherort ist im ersten Parameter der NODE-Anweisung in der PowerExchange-Konfigurationsdatei „dbmover.cfg“ angegeben.
PacingSize	Optional. Menge der Daten, die das Quellsystem an den PowerExchange-Listener weitergeben kann. Konfigurieren Sie die Pacing-Größe, wenn eine externe Anwendung, eine Datenbank oder der Datenintegrationsdienst einen Engpass darstellt. Je niedriger der Wert, umso schneller die Leistung. Der Mindestwert lautet 0. Geben Sie für maximale Leistung 0 ein. Standardwert ist 0.
RejectFile	Optional. Geben Sie den Namen und den Pfad der Ablehnungsdateien ein. Ablehnungsdateien enthalten Zeilen, die nicht in die Datenbank geschrieben wurden.
WriteMode	Geben Sie einen der folgenden Schreibmodi ein: <ul style="list-style-type: none"> <li>- CONFIRMWRITEON. Sendet Daten zum PowerExchange Listener und wartet auf eine Erfolgs-/Nichterfolgsreaktion, bevor weitere Daten gesendet werden.</li> <li>- CONFIRMWRITEOFF. Sendet Daten zum PowerExchange Listener, ohne eine Erfolgs-/Nichterfolgsreaktion abzuwarten. Verwenden Sie diese Option, wenn die Target-Tabelle bei Auftreten eines Fehlers erneut geladen werden kann.</li> <li>- ASYNCHRONOUSWITHFAULTT. Sendet Daten asynchron zum PowerExchange Listener mit der Möglichkeit der Fehlererkennung.</li> </ul> Der Standardwert ist CONFIRMWRITEON.
DatabaseFileOverrides	Gibt die i5/OS-Datenbankdateiüberschreibung an. Das Format ist: <code>from_file/to_library/to_file/to_member</code> Dabei gilt: <ul style="list-style-type: none"> <li>- <i>from_file</i> die zu überschreibende Datei ist</li> <li>- <i>to_library</i> die zu verwendende neue Bibliothek ist</li> <li>- <i>to_file</i> die zu verwendende Datei in der neuen Bibliothek ist</li> <li>- <i>to_member</i> optional ist und das zu verwendende Elemente in der neuen Bibliothek und Datei darstellt. *FIRST wird verwendet, wenn keine Angabe gemacht wird.</li> </ul> Sie können bis zu 8 eindeutige Dateiüberschreibungen für eine einzelne Verbindung angeben. Eine einfache Überschreibung gilt für eine einzelne Datei bzw. ein einzelnes Ziel. Wenn Sie mehr als eine Dateiüberschreibung angeben möchten, setzen Sie die Zeichenfolge der Dateiüberschreibungen in doppelte Anführungszeichen und nehmen Sie ein Leerzeichen zwischen den einzelnen Dateiüberschreibungen auf. <b>Hinweis:</b> Wenn sowohl LibraryList als auch DatabaseFileOverrides angegeben werden und eine Tabelle in beiden vorhanden ist, hat DatabaseFileOverrides Vorrang.
IsolationLevel	Commit-Bereich der Transaktion. Wählen Sie einen der folgenden Werte aus: <ul style="list-style-type: none"> <li>- Keine</li> <li>- CS. Cursorstabilität.</li> <li>- RR. Repeatable Read.</li> <li>- CHG. Ändern.</li> <li>- ALLE</li> </ul> Der Standardwert ist CS.

Option	Beschreibung
LibraryList	Liste der Bibliotheken, die PowerExchange durchsucht, um den Tabellennamen für die Anweisungen „Auswählen“, „Einfügen“, „Löschen“, „Aktualisieren“ zu bestimmen. PowerExchange durchsucht die Liste, wenn der Tabellename unvollständig ist. Trennen Sie Bibliotheken mit Kommas. <b>Hinweis:</b> Wenn sowohl LibraryList als auch DatabaseFileOverrides angegeben werden und eine Tabelle in beiden vorhanden ist, hat DatabaseFileOverrides Vorrang.
EnableConnectionPool	Optional. Ermöglicht Parallelverarbeitung beim Laden von Daten in eine Tabelle im Massenmodus. Wird für Oracle verwendet. „True“ oder „False“. Standardwert ist „True“.
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Datenintegrationsdienst für eine Datenbankverbindung aufrechterhält. Stellen Sie diesen Wert so ein, dass er größer als Mindestanzahl inaktiver Verbindungsinstanzen ist.
ConnectionPoolMaxIdleTime	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Standardwert ist 0.

## DB2 for z/OS-Verbindungsoptionen

Verwenden Sie DB2Z-Verbindungsoptionen, um die IBM für DB2 z/OS-Verbindung zu definieren.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die DB2Z-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
DataAccessConnectionString	Verbindungszeichenfolge für den Zugriff auf Daten in der Datenbank <Datenbankname>
EnvironmentSQL	Optional. SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt. <b>Hinweis:</b> Setzen Sie Sonderzeichen in doppelte Anführungszeichen.
CodePage	Erforderlich. Codepage, die zum Lesen aus einer Quelldatenbank oder zum Schreiben in eine Zieldatenbank oder -Datei verwendet wird.
ArraySize	Optional. Bestimmt die Anzahl der Datensätze im Speicher-Array für die Threads, wenn der Worker-Threads-Wert größer als 0 ist. Gültige Werte sind 1 bis 5000. Standardwert ist 25.

Option	Beschreibung
Komprimierung	Optional. Komprimiert die Daten, um die Menge an Daten zu reduzieren, die über das Netzwerk geschrieben werden. Standardwert ist „false“.
CorrelationID	Optional. Beschriftung, die auf DB2-Aufgaben oder -Abfragen angewendet wird, um DB2 for z/OS für die Ressource auszuweisen. Geben Sie bis zu 8 Byte an alphanumerischen Zeichen ein.
EncryptionLevel	Optional. Verschlüsselungsebene. Wenn Sie AES für die Option EncryptionType angeben, müssen Sie einen der folgenden Werte angeben, um die Ebene der AES-Verschlüsselung anzugeben: <ul style="list-style-type: none"> <li>- 1. Verwenden Sie einen 128-Bit-Verschlüsselungsschlüssel.</li> <li>- 2. Verwenden Sie einen 192-Bit-Verschlüsselungsschlüssel.</li> <li>- 3. Verwenden Sie einen 256-Bit-Verschlüsselungsschlüssel.</li> </ul> Standardwert ist 1. <b>Hinweis:</b> Wenn Sie für den Verschlüsselungstyp „Keine“ auswählen, ignoriert der Datenintegrationsdienst den Wert für die Verschlüsselungsebene.
EncryptionType	Optional. Steuert, ob Verschlüsselung verwendet werden soll. Geben Sie einen der folgenden Werte an: <ul style="list-style-type: none"> <li>- Keine</li> <li>- AES</li> </ul> Standardwert ist „Keine“.
InterpretAsRows	Optional. Repräsentiert die Pacing-Größe als Anzahl von Zeilen. Bei „false“ gibt die Pacing-Größe Kilobyte wieder. Standardwert ist „false“.
Speicherort:	Speicherort des PowerExchange Listenerknotens, der eine Verbindung zur Datenbank herstellen kann. Der Knoten wird in der dbmover.cfg-Konfigurationsdatei von PowerExchange definiert.
OffloadProcessing	Optional. Verschiebt die Stapeldatenverarbeitung von der VSAM-Quelle zum Datenintegrationsdienst-Computer. Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- Auto. Der Datenintegrationsdienst bestimmt, ob Offload-Verarbeitung verwendet werden soll.</li> <li>- Ja. Offload-Verarbeitung wird verwendet.</li> <li>- Nein. Offload-Verarbeitung wird nicht verwendet.</li> </ul> Standardwert ist „Auto“.
PacingSize	Optional. Menge der Daten, die das Quellsystem an den PowerExchange-Listener weitergeben kann. Konfigurieren Sie die Pacing-Größe, wenn eine externe Anwendung, eine Datenbank oder der Datenintegrationsdienst einen Engpass darstellt. Je niedriger der Wert, umso schneller die Leistung. Der Mindestwert lautet 0. Geben Sie für maximale Leistung 0 ein. Standardwert ist 0.
RejectFile	Optional. Geben Sie den Namen und den Pfad der Ablehnungsdateien ein. Ablehnungsdateien enthalten Zeilen, die nicht in die Datenbank geschrieben wurden.
WorkerThread	Optional. Anzahl der vom Datenintegrationsdienst verwendeten Threads, um Stapeldaten bei aktivierter Offload-Verarbeitung zu verarbeiten. Um eine optimale Leistung zu erzielen, sollte dieser Wert die Anzahl der verfügbaren Prozessoren auf dem Rechner des Datenintegrationsdienstes nicht überschreiten. Gültige Werte sind 1 bis 64. Standardwert ist 0, wodurch Multithreading deaktiviert wird.

Option	Beschreibung
WriteMode	Geben Sie einen der folgenden Schreibmodi ein: <ul style="list-style-type: none"> <li>- CONFIRMWRITEON. Sendet Daten zum PowerExchange Listener und wartet auf eine Erfolgs-/Nichterfolgsreaktion, bevor weitere Daten gesendet werden.</li> <li>- CONFIRMWRITEOFF. Sendet Daten zum PowerExchange Listener, ohne eine Erfolgs-/Nichterfolgsreaktion abzuwarten. Verwenden Sie diese Option, wenn die Target-Tabelle bei Auftreten eines Fehlers erneut geladen werden kann.</li> <li>- ASYNCHRONOUSWITHFAULTT. Sendet Daten asynchron zum PowerExchange Listener mit der Möglichkeit der Fehlererkennung.</li> </ul> Der Standardwert ist CONFIRMWRITEON.
EnableConnectionPool	Optional. Ermöglicht Parallelverarbeitung beim Laden von Daten in eine Tabelle im Massenmodus. Wird für Oracle verwendet. „True“ oder „False“. Standardwert ist „True“.
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Datenintegrationsdienst für eine Datenbankverbindung aufrechterhält. Stellen Sie diesen Wert so ein, dass er größer als Mindestanzahl inaktiver Verbindungsinstanzen ist.
ConnectionPoolMaxIdleTime	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Standardwert ist 0.

## Facebook-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Facebook-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Facebook-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
ConsumerKey	Die Anwendungs-ID, die Sie beim Erstellen der Anwendung in Facebook erhalten. Facebook verwendet den Schlüssel zur Identifizierung der Anwendung.
ConsumerSecret	Das Anwendungsgeheimwort, das Sie beim Erstellen der Anwendung in Facebook erhalten. Facebook verwendet das Geheimwort für das Eigentum am Verbraucherschlüssel.
AccessToken	Zugriffstoken, den das OAuth-Dienstprogramm zurückgibt. Facebook verwendet diesen Token anstelle der Benutzeranmeldedaten für den Zugriff auf geschützte Ressourcen.

Option	Beschreibung
AccessSecret	Das Zugriffsgeheimwort ist für eine Facebook-Verbindung nicht erforderlich.
Bereich	Berechtigungen für die Anwendung. Geben Sie die Berechtigungen ein, die Sie zum Konfigurieren von OAuth verwendet haben.

## Greenplum-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Greenplum-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

... -o option\_name=value option\_name=value ...

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Greenplum-Verbindungsoptionen für die `infacmd` `isp` `CreateConnection`- und `UpdateConnection`-Befehle beschrieben:

Option	Beschreibung
UserName	Erforderlich. Benutzername mit Berechtigungen für den Zugriff auf die Greenplum-Datenbank.
Passwort	Erforderlich. Passwort für die Verbindung zur Greenplum-Datenbank.
driverName	Erforderlich. Name des Greenplum-JDBC-Treibers. Beispiel: <code>com.pivotal.jdbc.GreenplumDriver</code> Weitere Informationen über den Treiber finden Sie in der Greenplum-Dokumentation.
connectionString	Erforderlich. Greenplum-JDBC-Verbindungs-URL. Beispiel: <code>jdbc:pivotal:greenplum://&lt;hostname&gt;:&lt;port&gt;;DatabaseName=&lt;database_name&gt;</code> Weitere Informationen über die Verbindungs-URL finden Sie in der Greenplum-Dokumentation.
hostName	Erforderlich. Hostname oder IP-Adresse des Greenplum-Servers.
portNumber	Optional. Portnummer des Greenplum-Servers. Wenn Sie 0 eingeben, liest das Dienstprogramm „gpload“ aus der Umgebungsvariable <code>\$PGPORT</code> . Standardwert ist 5432.
databaseName	Erforderlich. Name der Datenbank, zu der Sie eine Verbindung herstellen möchten.
enableSSL	Erforderlich. Legen Sie diese Option auf <code>TRUE</code> fest, um sichere Kommunikation zwischen dem Dienstprogramm „gpload“ und dem Greenplum-Server über SSL einzurichten.
SSLCertificatePath	Erforderlich, wenn Sie SSL aktivieren. Pfad, in dem die SSL-Zertifikate für den Greenplum-Server gespeichert werden.

## Google Analytics-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren der Google Analytics-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Beispiel:

```
./infacmd.sh createconnection -dn Domain_Google -un Administrator -pd Administrator -cn  
GA_cmd -ct GOOGLEANALYTICS -o "SERVICEACCOUNTID=serviceaccount@api-  
project-12345.iam.gserviceaccount.com SERVICEACCOUNTKEY='---BEGIN PRIVATE KEY---  
\nabcd1234322dsa\n---END PRIVATE KEY---\n' PROJECTID=api-project-12333667"
```

In der folgenden Tabelle werden die Google Analytics-Verbindungsoptionen für die Befehle „infacmd isp CreateConnection“ und „UpdateConnection“ beschrieben:

Eigenschaft	Beschreibung
SERVICEACCOUNTID	Erforderlich. Gibt den Wert „client_email“ an, der in der JSON-Datei enthalten ist, die Sie nach dem Erstellen eines Dienstkontos herunterladen.
SERVICEACCOUNTKEY	Erforderlich. Gibt den Wert „private_key“ an, der in der JSON-Datei enthalten ist, die Sie nach dem Erstellen eines Dienstkontos herunterladen.

## Google BigQuery-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren der Google BigQuery-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Beispiel:

```
./infacmd.sh createconnection -dn Domain_Adapters_1041_Uni -un Administrator -pd  
Administrator -cn GBQ_BDM -ct BIGQUERY -o "CLIENTEMAIL='ics-test@api-  
project-80697026669.iam.gserviceaccount.com' PRIVATEKEY='-----BEGIN PRIVATE KEY-----  
\nMIIGfdzhgy74587igu787tio9QEFAASCBKgwggSkAgEAAoIBAQCy+2Dbh\n-----END PRIVATE KEY-----  
\n' PROJECTID=api-project-86699686669 CONNECTORTYPE=Simple SCHEMALOCATION='gs://0_europe-  
west6_region' STORAGEPATH='gs://0_europe-west6_region'  
DATASETNAMEFORCUSTOMQUERY='europe_west6' REGIONID='europe-west6' " ;
```

In der folgenden Tabelle werden die Google BigQuery-Verbindungsoptionen für die Befehle „infacmd isp CreateConnection“ und „UpdateConnection“ beschrieben:

Eigenschaft	Beschreibung
CLIENTEMAIL	Erforderlich. Gibt den Wert von „client_email“ in der JSON-Datei an, die Sie nach dem Erstellen eines Dienstkontos in Google BigQuery herunterladen.
PRIVATEKEY	Erforderlich. Gibt den Wert von „private_key“ in der JSON-Datei an, die Sie nach dem Erstellen eines Dienstkontos in Google BigQuery herunterladen.

Eigenschaft	Beschreibung
Verbindungsmodus CONNECTORTYPE	<p>Erforderlich. Der Verbindungsmodus, der zum Lesen von Daten aus oder Schreiben von Daten in Google BigQuery verwendet werden soll.</p> <p>Geben Sie einen der folgenden Verbindungsmodi ein:</p> <ul style="list-style-type: none"> <li>- Einfach. Enthierarchisiert jedes Feld innerhalb des Felds mit dem Datentyp „Datensatz“ als separates Feld im Mapping.</li> <li>- Hybrid. Zeigt alle Felder der obersten Ebene in der Google BigQuery-Tabelle an, einschließlich der Felder mit dem Datentyp „Datensatz“. PowerExchange for Google BigQuery zeigt das Feld der obersten Ebene mit dem Datentyp „Datensatz“ im Mapping als einzelnes Feld mit dem Datentyp „Zeichenfolge“ an.</li> <li>- Komplex. Zeigt alle Spalten in der Google BigQuery-Tabelle als einzelnes Feld mit dem Datentyp „Zeichenfolge“ im Mapping an.</li> </ul> <p>Der Standardwert ist „Einfach“.</p>
Dateipfad für die Schemadefinition SCHEMALOCATION	<p>Erforderlich. Gibt ein Verzeichnis auf dem Clientcomputer an, in dem PowerExchange for Google BigQuery eine JSON-Datei mit dem Beispielschema der Google BigQuery-Tabelle erstellen muss. Der Name der JSON-Datei ist der gleiche wie der Name der Google BigQuery-Tabelle.</p> <p>Alternativ können Sie einen Speicherpfad in Google Cloud Storage eingeben, in dem PowerExchange for Google BigQuery eine JSON-Datei mit dem Beispielschema der Google BigQuery-Tabelle erstellen muss. Sie können die JSON-Datei vom angegebenen Speicherpfad in Google Cloud Storage auf einen lokalen Computer herunterladen.</p>
PROJECTID	<p>Erforderlich. Gibt den Wert von „project_id“ in der JSON-Datei an, die Sie nach dem Erstellen eines Dienstkontos in Google BigQuery herunterladen.</p> <p>Wenn Sie mehrere Projekte mit demselben Dienstkonto erstellt haben, geben Sie die ID des Projekts ein, das den Datensatz enthält, zu der Sie eine Verbindung herstellen möchten.</p>
STORAGEPATH	<p>Erforderlich, wenn große Datenmengen gelesen oder geschrieben werden sollen.</p> <p>Pfad in Google Cloud Storage, in dem PowerExchange for Google BigQuery eine lokale Speicherdatei zum vorübergehenden Speichern der Daten erstellt.</p> <p>Sie können entweder den Bucket-Namen oder den Bucket-Namen und den Ordernamen eingeben.</p> <p>Geben Sie beispielsweise <code>gs://&lt;Bucket-Name&gt;</code> oder <code>gs://&lt;Bucket-Name&gt;/&lt;Ordnername&gt;</code> ein.</p>
REGIONID	<p>Der Name der Region, in der sich der Google BigQuery-Datensatz befindet.</p> <p>Wenn Sie beispielsweise eine Verbindung zu einem in der Region Las Vegas gespeicherten Google BigQuery-Datensatz herstellen möchten, geben Sie <b>us-west4</b> als <b>Regions-ID</b> an.</p> <p><b>Hinweis:</b> Stellen Sie sicher, dass Sie in der Verbindungseigenschaft <b>Speicherpfad</b> einen Bucket-Namen oder den Bucket-Namen und den Ordernamen angeben, der bzw. die sich in derselben Region befinden wie der Datensatz in Google BigQuery.</p> <p>Weitere Informationen zu den von Google BigQuery unterstützten Regionen finden Sie in der folgenden Google BigQuery-Dokumentation: <a href="https://cloud.google.com/bigquery/docs/locations">https://cloud.google.com/bigquery/docs/locations</a>.</p>

## Google Cloud Spanner-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren der Google Cloud Spanner-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.



Beispiel:

```
./infacmd.sh createconnection dn Domain Google -un Administrator -pd Administrator -cn  
Spanner_cmd -ct SPANNERGOOGLE -o "CLIENTEMAIL=serviceaccount@api-  
project-12345.iam.gserviceaccount.com PRIVATEKEY='---BEGIN PRIVATE KEY---\nabcd1234322dsa  
\n---END PRIVATE KEY---\n' INSTANCEID=spanner-testing PROJECTID=api-project-12333667"
```

In der folgenden Tabelle werden die Google Cloud Spanner-Verbindungsoptionen für die Befehle „infacmd isp CreateConnection“ und „UpdateConnection“ beschrieben:

Eigenschaft	Beschreibung
CLIENTEMAIL	Erforderlich. Gibt den Wert „client_email“ an, der in der JSON-Datei enthalten ist, die Sie nach dem Erstellen eines Dienstkontos in Google Cloud Spanner herunterladen.
PRIVATEKEY	Erforderlich. Gibt den Wert „private_key“ an, der in der JSON-Datei enthalten ist, die Sie nach dem Erstellen eines Dienstkontos in Google Cloud Spanner herunterladen.
PROJECTID	Erforderlich. Gibt den Wert „project_id“ an, der in der JSON-Datei enthalten ist, die Sie nach dem Erstellen eines Dienstkontos in Google Cloud Spanner herunterladen.  Wenn Sie mehrere Projekte mit demselben Dienstkonto erstellt haben, geben Sie die ID des Projekts mit dem Datensatz ein, zu dem Sie eine Verbindung herstellen möchten.
INSTANCEID	Erforderlich. Name der in Google Cloud Spanner erstellten Instanz.

## Google Cloud Storage-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren der Google Cloud Storage-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Beispiel:

```
./infacmd.sh createconnection dn Domain Google -un Administrator -pd Administrator -cn  
GCS_cmd -ct GOOGLESTORAGEV2 -o "CLIENTEMAIL=serviceaccount@api-  
project-12345.iam.gserviceaccount.com PRIVATEKEY='---BEGIN PRIVATE KEY---\nabcd1234322dsa  
\n---END PRIVATE KEY---\n' PROJECTID=api-project-12333667"
```

In der folgenden Tabelle werden die Google Cloud Storage-Verbindungsoptionen für die Befehle „infacmd isp CreateConnection“ und „UpdateConnection“ beschrieben:

Eigenschaft	Beschreibung
CLIENTEMAIL	Erforderlich. Gibt den Wert „client_email“ an, der in der JSON-Datei enthalten ist, die Sie nach dem Erstellen eines Dienstkontos herunterladen.
PRIVATEKEY	Erforderlich. Gibt den Wert „private_key“ an, der in der JSON-Datei enthalten ist, die Sie nach dem Erstellen eines Dienstkontos herunterladen.
PROJECTID	Erforderlich. Gibt den Wert „project_id“ an, der in der JSON-Datei enthalten ist, die Sie nach dem Erstellen eines Dienstkontos herunterladen.  Wenn Sie mehrere Projekte mit demselben Dienstkonto erstellt haben, geben Sie die ID des Projekts mit dem Bucket ein, zu dem Sie eine Verbindung herstellen möchten.

## Hadoop Connection Options

Use connection options to define a Hadoop connection.

Enter connection options in the following format:

```
... -o option_name='value' option_name='value' ...
```

To enter multiple options, separate them with a space.

To enter advanced properties, use the following format:

```
... -o engine_nameAdvancedProperties="'advanced.property.name=value'"
```

For example:

```
... -o blazeAdvancedProperties="'infrgrid.orchestrator.svc.sunset.time=3'"
```

The following table describes Hadoop connection options for infacmd isp CreateConnection and UpdateConnection commands that you configure when you want to use the Hadoop connection:

Option	Description
connectionId	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
connectionType	Required. Type of connection is Hadoop.
name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { [ ]   \ : ; " ' < , > . ? /
blazeJobMonitorURL	The host name and port number for the Blaze Job Monitor. Use the following format: <hostname>:<port> Where - <hostname> is the host name or IP address of the Blaze Job Monitor server. - <port> is the port on which the Blaze Job Monitor listens for remote procedure calls (RPC). For example, enter: myhostname:9080
blazeYarnQueueName	The YARN scheduler queue name used by the Blaze engine that specifies available resources on a cluster. The name is case sensitive.
blazeAdvancedProperties	Advanced properties that are unique to the Blaze engine. To enter multiple properties, separate each name-value pair with the following text: &:. Use Informatica custom properties only at the request of Informatica Global Customer Support.
blazeMaxPort	The maximum value for the port number range for the Blaze engine. Default value is 12600
blazeMinPort	The minimum value for the port number range for the Blaze engine. Default value is 12300

Option	Description
blazeUserName	The owner of the Blaze service and Blaze service logs. When the Hadoop cluster uses Kerberos authentication, the default user is the Data Integration Service SPN user. When the Hadoop cluster does not use Kerberos authentication and the Blaze user is not configured, the default user is the Data Integration Service user.
blazeStagingDirectory	The HDFS file path of the directory that the Blaze engine uses to store temporary files. Verify that the directory exists. The YARN user, Blaze engine user, and mapping impersonation user must have write permission on this directory. Default is <code>/blaze/workdir</code> . If you clear this property, the staging files are written to the Hadoop staging directory <code>/tmp/blaze_&lt;user name&gt;</code> .
clusterConfigId	The cluster configuration ID associated with the Hadoop cluster. You must enter a configuration ID to set up a Hadoop connection.
hiveStagingDatabaseName	Namespace for Hive staging tables. Use the name <code>default</code> for tables that do not have a specified database name.
engineType	Execution engine to run HiveServer2 tasks on the Spark engine. Default is MRv2. You can choose MRv2 or Tez according to the engine type that the Hadoop distribution uses: <ul style="list-style-type: none"> <li>- Amazon EMR. Tez</li> <li>- Azure HDI. Tez</li> <li>- Cloudera CDH. MRv2</li> <li>- Cloudera CDP. Tez</li> <li>- Dataproc. MRv2</li> <li>- Hortonworks HDP. Tez</li> <li>- MapR. MRv2</li> </ul>
environmentsSQL	SQL commands to set the Hadoop environment. The Data Integration Service executes the environment SQL at the beginning of each Hive script generated in a Hive execution plan. The following rules and guidelines apply to the usage of environment SQL: <ul style="list-style-type: none"> <li>- Use the environment SQL to specify Hive queries.</li> <li>- Use the environment SQL to set the classpath for Hive user-defined functions and then use environment SQL or PreSQL to specify the Hive user-defined functions. You cannot use PreSQL in the data object properties to specify the classpath. If you use Hive user-defined functions, you must copy the .jar files to the following directory: <code>&lt;Informatica installation directory&gt;/services/shared/hadoop/&lt;Hadoop distribution name&gt;/extras/hive-auxjars</code></li> <li>- You can use environment SQL to define Hadoop or Hive parameters that you want to use in the PreSQL commands or in custom queries.</li> </ul>
hadoopExecEnvExecutionParameterList	Custom properties that are unique to the Hadoop connection. You can specify multiple properties. Use the following format: <code>&lt;property1&gt;=&lt;value&gt;</code> To specify multiple properties use <code>&amp; :</code> as the property separator. If more than one Hadoop connection is associated with the same cluster configuration, you can override configuration set property values. Use Informatica custom properties only at the request of Informatica Global Customer Support.

Option	Description
hadoopRejDir	<p>The remote directory where the Data Integration Service moves reject files when you run mappings.</p> <p>Enable the reject directory using rejDirOnHadoop.</p>
impersonationUserName	<p>Required if the Hadoop cluster uses Kerberos authentication. Hadoop impersonation user. The user name that the Data Integration Service impersonates to run mappings in the Hadoop environment.</p> <p>The Data Integration Service runs mappings based on the user that is configured. Refer the following order to determine which user the Data Integration Services uses to run mappings:</p> <ol style="list-style-type: none"> <li>1. Operating system profile user. The mapping runs with the operating system profile user if the profile user is configured. If there is no operating system profile user, the mapping runs with the Hadoop impersonation user.</li> <li>2. Hadoop impersonation user. The mapping runs with the Hadoop impersonation user if the operating system profile user is not configured. If the Hadoop impersonation user is not configured, the Data Integration Service runs mappings with the Data Integration Service user.</li> <li>3. Data Integration Service user. The mapping runs with the Data Integration Service user if the operating system profile user and the Hadoop impersonation user are not configured.</li> </ol>
hiveWarehouseDirectoryOnHDFS	<p>Optional. The absolute HDFS file path of the default database for the warehouse that is local to the cluster.</p> <p>If you do not configure the Hive warehouse directory, the Hive engine first tries to write to the directory specified in the cluster configuration property <code>hive.metastore.warehouse.dir</code>. If the cluster configuration does not have the property, the Hive engine writes to the default directory <code>/user/hive/warehouse</code>.</p>
metastoreDatabaseDriver	<p>Driver class name for the JDBC data store. For example, the following class name specifies a MySQL driver:</p> <pre>com.mysql.jdbc.Driver</pre> <p>You can get the value for the Metastore Database Driver from <code>hive-site.xml</code>. The Metastore Database Driver appears as the following property in <code>hive-site.xml</code>:</p> <pre>&lt;property&gt;   &lt;name&gt;javax.jdo.option.ConnectionDriverName&lt;/name&gt;   &lt;value&gt;com.mysql.jdbc.Driver&lt;/value&gt; &lt;/property&gt;</pre>
metastoreDatabasePassword	<p>The password for the metastore user name.</p> <p>You can get the value for the Metastore Database Password from <code>hive-site.xml</code>. The Metastore Database Password appears as the following property in <code>hive-site.xml</code>:</p> <pre>&lt;property&gt;   &lt;name&gt;javax.jdo.option.ConnectionPassword&lt;/name&gt;   &lt;value&gt;password&lt;/value&gt; &lt;/property&gt;</pre>

Option	Description
metastoreDatabaseURI	<p>The JDBC connection URI used to access the data store in a local metastore setup. Use the following connection URI:</p> <pre>jdbc:&lt;datastore type&gt;://&lt;node name&gt;:&lt;port&gt;/&lt;database name&gt;</pre> <p>where</p> <ul style="list-style-type: none"> <li>- &lt;node name&gt; is the host name or IP address of the data store.</li> <li>- &lt;data store type&gt; is the type of the data store.</li> <li>- &lt;port&gt; is the port on which the data store listens for remote procedure calls (RPC).</li> <li>- &lt;database name&gt; is the name of the database.</li> </ul> <p>For example, the following URI specifies a local metastore that uses MySQL as a data store:</p> <pre>jdbc:mysql://hostname23:3306/metastore</pre> <p>You can get the value for the Metastore Database URI from hive-site.xml. The Metastore Database URI appears as the following property in hive-site.xml:</p> <pre>&lt;property&gt;   &lt;name&gt;javax.jdo.option.ConnectionURL&lt;/name&gt;   &lt;value&gt;jdbc:mysql://MYHOST/metastore&lt;/value&gt; &lt;/property&gt;</pre>
metastoreDatabaseUserName	<p>The metastore database user name.</p> <p>You can get the value for the Metastore Database User Name from hive-site.xml. The Metastore Database User Name appears as the following property in hive-site.xml:</p> <pre>&lt;property&gt;   &lt;name&gt;javax.jdo.option.ConnectionUserName&lt;/name&gt;   &lt;value&gt;hiveuser&lt;/value&gt; &lt;/property&gt;</pre>
metastoreMode	<p>Controls whether to connect to a remote metastore or a local metastore. By default, local is selected. For a local metastore, you must specify the Metastore Database URI, Metastore Database Driver, Username, and Password. For a remote metastore, you must specify only the Remote Metastore URI.</p> <p>You can get the value for the Metastore Execution Mode from hive-site.xml. The Metastore Execution Mode appears as the following property in hive-site.xml:</p> <pre>&lt;property&gt; &lt;name&gt;hive.metastore.local&lt;/name&gt; &lt;value&gt;true&lt;/true&gt; &lt;/property&gt;</pre> <p><b>Hinweis:</b> The <code>hive.metastore.local</code> property is deprecated in hive-site.xml for Hive server versions 0.9 and above. If the <code>hive.metastore.local</code> property does not exist but the <code>hive.metastore.uris</code> property exists, and you know that the Hive server has started, you can set the connection to a remote metastore.</p>

Option	Description
remoteMetastoreURI	<p>The metastore URI used to access metadata in a remote metastore setup. For a remote metastore, you must specify the Thrift server details.</p> <p>Use the following connection URI: thrift://&lt;hostname&gt;:&lt;port&gt;</p> <p>Where</p> <ul style="list-style-type: none"> <li>- &lt;hostname&gt; is name or IP address of the Thrift metastore server.</li> <li>- &lt;port&gt; is the port on which the Thrift server is listening.</li> </ul> <p>For example, enter: thrift://myhostname:9083/</p> <p>You can get the value for the Remote Metastore URI from hive-site.xml. The Remote Metastore URI appears as the following property in hive-site.xml:</p> <pre>&lt;property&gt;   &lt;name&gt;hive.metastore.uris&lt;/name&gt;   &lt;value&gt;thrift://&lt;n.n.n.n&gt;:9083&lt;/value&gt; &lt;description&gt; IP address or fully-qualified domain name and port of the metastore host&lt;/description&gt; &lt;/property&gt;</pre>
rejDirOnHadoop	<p>Enables hadoopRejDir. Used to specify a location to move reject files when you run mappings.</p> <p>If enabled, the Data Integration Service moves mapping files to the HDFS location listed in hadoopRejDir.</p> <p>By default, the Data Integration Service stores the mapping files based on the RejectDir system parameter.</p>
sparkEventLogDir	Optional. The HDFS file path of the directory that the Spark engine uses to log events.
sparkAdvancedProperties	<p>Advanced properties that are unique to the Spark engine.</p> <p>To enter multiple properties, separate each name-value pair with the following text: &amp;:.</p> <p>Use Informatica custom properties only at the request of Informatica Global Customer Support.</p>
sparkStagingDirectory	<p>The HDFS file path of the directory that the Spark engine uses to store temporary files for running jobs. The YARN user, Data Integration Service user, and mapping impersonation user must have write permission on this directory.</p> <p>By default, the temporary files are written to the Hadoop staging directory /tmp/spark_&lt;user name&gt;.</p>
sparkYarnQueueName	The YARN scheduler queue name used by the Spark engine that specifies available resources on a cluster. The name is case sensitive.
stgDataCompressionCodecClasses	Codec class name that enables data compression and improves performance on temporary staging tables. The codec class name corresponds to the code type.
stgDataCompressionCodecType	<p>Hadoop compression library for a compression codec class name.</p> <p>You can choose None, Zlib, Gzip, Snappy, Bz2, LZ0, or Custom.</p> <p>Default is None.</p>

## HBase-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer HBase-Verbindung. Sie können eine HBase-Verbindung verwenden, um eine Verbindung mit einer HBase-Tabelle oder einer MapR-DB-Tabelle herzustellen.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die HBase-Verbindungsoptionen für die Befehle „`infacmd isp CreateConnection`“ und „`UpdateConnection`“ beschrieben:

Option	Beschreibung
DATABASETYPE	Erforderlich, wenn Sie eine HBase-Verbindung für eine MapR-DB-Tabelle erstellen. Legen Sie den Wert auf MapR-DB fest. Standard ist HBase.
clusterConfigId	The cluster configuration ID associated with the Hadoop cluster. You must enter a configuration ID to set up a Hadoop connection.
maprdbpath	<p>Erforderlich, wenn Sie eine HBase-Verbindung erstellen, um eine Verbindung zu einer MapR-DB-Tabelle herzustellen.</p> <p>Legen Sie den Wert auf den Datenbankpfad fest, der die MapR-DB-Tabelle enthält, mit der Sie eine Verbindung herstellen möchten. Geben Sie einen gültigen MapR-Clusterpfad ein. Schließen Sie den Wert in einfache Anführungszeichen ein.</p> <p>Wenn Sie ein HBase-Datenobjekt für MapR-DB erstellen, können Sie nur Tabellen durchsuchen, die in dem in dieser Option angegebenen Pfad vorhanden sind. Sie können nicht auf Tabellen zugreifen, die in Unterverzeichnissen im angegebenen Pfad verfügbar sind.</p> <p>Wenn Sie z. B. als <code>maprdbpath</code> den Pfad <code>/user/customers/</code> angeben, können Sie auf die Tabellen im Verzeichnis <code>customers</code> zugreifen. Wenn das Verzeichnis <code>customers</code> jedoch ein Unterverzeichnis mit dem Namen <code>regions</code> enthält, können Sie nicht auf die Tabellen im folgenden Verzeichnis zugreifen:</p> <p><code>/user/customers/regions</code></p>

## HDFS-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer HDFS-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die HDFS-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
userName	Benutzername für den Zugriff auf HDFS.
nameNodeURI	Der URI für den Zugriff auf das Speichersystem. Der Wert für <code>fs.defaultFS</code> befindet sich im Konfigurationssatz <code>core-site.xml</code> der Cluster-Konfiguration.
clusterConfigId	The cluster configuration ID associated with the Hadoop cluster. You must enter a configuration ID to set up a Hadoop connection.

## Hive-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Hive-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name='value' option_name='value' ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen.

Die folgende Tabelle beschreibt Hive-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle, die Sie konfigurieren, wenn Sie die Hive-Verbindung verwenden möchten:

Option	Beschreibung
connectionType	Erforderlich. Verbindungstyp ist HIVE.
name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * ( ) - + = { [ } ]   \ : ; " ' < , > . ? /



Option	Beschreibung
environmentSQL	<p>SQL-Befehle zum Einrichten der Hadoop-Umgebung. Im nativen Umgebungstyp führt der Datenintegrationsdienst die Umgebungs-SQL jedes Mal aus, wenn er eine Verbindung zum Hive-Metastore herstellt. Wenn die Hive-Verbindung zum Ausführen von Mappings im Hadoop-Cluster verwendet wird, führt der Datenintegrationsdienst die Umgebungs-SQL am Anfang jeder Hive-Sitzung aus.</p> <p>Die folgenden Regeln und Richtlinien gelten für die Verwendung von Umgebungs-SQL in beiden Verbindungsmodi:</p> <ul style="list-style-type: none"> <li>- Verwenden Sie die Umgebungs-SQL, um Hive-Abfragen anzugeben.</li> <li>- Verwenden Sie die Umgebungs-SQL, um den Klassenpfad für benutzerdefinierte Hive-Funktionen einzustellen und verwenden Sie dann entweder Umgebungs-SQL oder PreSQL, um die benutzerdefinierten Hive-Funktionen anzugeben. Sie können PreSQL nicht in den Datenobjekteigenschaften zur Angabe des Klassenpfads verwenden. Wenn Sie benutzerdefinierte Hive-Funktionen verwenden, müssen Sie die JAR-Dateien in das folgende Verzeichnis kopieren:</li> </ul> <pre>&lt;Informatica-Installationsverzeichnis&gt;/services/shared/hadoop/&lt;Name der Hadoop-Distribution&gt;/extras/hive-auxjars</pre> <ul style="list-style-type: none"> <li>- Sie können auch Umgebungs-SQL zum Definieren von Hadoop- oder Hive-Parametern verwenden, die Sie in den PreSQL-Befehlen oder in benutzerspezifischen Abfragen nutzen möchten.</li> </ul> <p>Wenn die Hive-Verbindung zum Ausführen von Mappings im Hadoop-Cluster verwendet wird, wird nur die Umgebungs-SQL der Hive-Verbindung ausgeführt. Die verschiedenen Umgebungs-SQL-Befehle für die Verbindungen von Hive-Quelle oder -Ziel werden nicht ausgeführt, selbst wenn sich Hive-Quellen und -Ziele in verschiedenen Clustern befinden.</p>
quoteChar	<p>Der Zeichentyp, der zur Kennzeichnung von Sonderzeichen und reservierten SQL-Schlüsselwörtern, wie WHERE, verwendet wird. Der Datenintegrationsdienst schließt mit dem ausgewählten Zeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Außerdem nutzt der Datenintegrationsdienst dieses Zeichen für die Eigenschaft <b>Unterstützte IDs mit gemischter Groß-/Kleinschreibung</b>.</p>
clusterConfigId	<p>The cluster configuration ID associated with the Hadoop cluster. You must enter a configuration ID to set up a Hadoop connection.</p>

## Eigenschaften für den Zugriff auf Hive als Quelle oder Ziel

Die folgende Tabelle beschreibt die erforderlichen Optionen für infacmd isp CreateConnection- und UpdateConnection-Befehle, die Sie konfigurieren, wenn Sie die Hive-Verbindung für den Zugriff auf Daten verwenden möchten:

Eigenschaft	Beschreibung
hiveJdbcDriverClassName	Name der JDBC-Treiberklasse.
metadataConnString	<p>Der JDBC-Verbindungs-URI für den Zugriff auf die Metadaten des Hadoop-Servers. Die Verbindungszeichenfolge verwendet das folgende Format:</p> <pre>jdbc:hive://&lt;hostname&gt;:&lt;port&gt;/&lt;db&gt;</pre> <p>Wobei</p> <ul style="list-style-type: none"><li>- <code>hostname</code> der Name oder die IP-Adresse des Rechners ist, auf dem der Hive-Server ausgeführt wird</li><li>- <code>port</code> der Port ist, auf dem der Hive-Server abhört</li><li>- <code>db</code> die Datenbank ist, zu der Sie eine Verbindung herstellen möchten. Wenn Sie die Datenbankdetails nicht zur Verfügung stellen, verwendet der Datenintegrationsdienst die standardmäßigen Datenbank-Details.</li></ul> <p>Zum Herstellen einer Verbindung zu HiveServer 2 verwenden Sie das Verbindungsstringformat, das Apache Hive für diese bestimmte Hadoop-Verteilung implementiert. Weitere Informationen über Apache Hive-Verbindungsstringformate finden Sie in der Apache Hive-Dokumentation.</p> <p>Wenn der Hadoop-Cluster SSL- oder TLS-Authentifizierung verwendet, müssen Sie dem JDBC-Verbindungs-URI <code>ssl=true</code> hinzufügen. Beispiel: <code>jdbc:hive2://&lt;Hostname&gt;:&lt;Port&gt;/&lt;db&gt;;ssl=true</code></p> <p>Wenn Sie selbstsignierte Zertifikate für die SSL- oder TLS-Authentifizierung verwenden, stellen Sie sicher, dass die Zertifikatsdatei auf dem Client- und dem Datenintegrationsdienst-Computer verfügbar ist. Weitere Informationen finden Sie im <i>Informatica Big Data Management-Cluster-Integrationshandbuch</i>.</p>
bypassHiveJDBCServer	<p>JDBC-Treibermodus. Aktivieren Sie diese Option zur Verwendung des eingebetteten JDBC-Treibers (eingebetteter Modus).</p> <p>Zur Verwendung des eingebetteten JDBC-Modus führen Sie folgende Aufgaben durch:</p> <ul style="list-style-type: none"><li>- Stellen Sie sicher, dass Hive-Client und Informatica-Dienste auf demselben Rechner installiert sind.</li><li>- Konfigurieren Sie die Hive-Verbindungseigenschaften zum Ausführen von Mappings im Hadoop-Cluster.</li></ul> <p>Wenn Sie den nicht eingebetteten Modus wählen, müssen Sie den Verbindungszeichenfolge für Datenzugriff konfigurieren.</p> <p>Der eingebettete JDBC-Modus wird dem nicht eingebetteten Modus vorgezogen.</p>

Eigenschaft	Beschreibung
sqlAuthorized	<p>Wenn Sie die Option auswählen, um differenzierte SQL-Authentifizierung in einer Hive-Quelle zu berücksichtigen, berücksichtigt das Mapping Einschränkungen für den Datenzugriff auf Zeilen- und Spaltenebene. Wenn Sie die Option nicht auswählen, ignoriert die Blaze-Laufzeit-Engine die Einschränkungen, und die Ergebnisse enthalten eingeschränkte Daten.</p> <p>Anwendbar auf Hadoop-Cluster, in denen die Sicherheitsmodi „Sentry“ oder „Ranger“ aktiviert sind.</p>
connectString	<p>Die Verbindungszeichenfolge, die zum Zugriff auf Daten aus dem Hadoop-Datenspeicher verwendet wird. Die Verbindungszeichenfolge des nicht eingebetteten JDBC-Modus muss das folgende Format haben:</p> <pre>jdbc:hive://&lt;hostname&gt;:&lt;port&gt;/&lt;db&gt;</pre> <p>Wobei</p> <ul style="list-style-type: none"> <li>- <code>hostname</code> der Name oder die IP-Adresse des Rechners ist, auf dem der Hive-Server ausgeführt wird.</li> <li>- <code>port</code> der Port ist, auf dem der Hive-Server abhört. Der Standardwert ist 10000.</li> <li>- <code>db</code> die Datenbank ist, zu der Sie eine Verbindung herstellen möchten. Wenn Sie die Datenbankdetails nicht zur Verfügung stellen, verwendet der Datenintegrationsdienst die standardmäßigen Datenbank-Details.</li> </ul> <p>Zum Herstellen einer Verbindung zu HiveServer 2 verwenden Sie das Verbindungsstringformat, das Apache Hive für diese bestimmte Hadoop-Verteilung implementiert. Weitere Informationen über Apache Hive-Verbindungsstringformate finden Sie in der Apache Hive-Dokumentation.</p> <p>Wenn der Hadoop-Cluster SSL- oder TLS-Authentifizierung verwendet, müssen Sie dem JDBC-Verbindungs-URI <code>ssl=true</code> hinzufügen. Beispiel: <code>jdbc:hive2://&lt;Hostname&gt;:&lt;Port&gt;/&lt;db&gt;;ssl=true</code></p> <p>Wenn Sie selbstsignierte Zertifikate für die SSL- oder TLS-Authentifizierung verwenden, stellen Sie sicher, dass die Zertifikatsdatei auf dem Client- und dem Datenintegrationsdienst-Computer verfügbar ist. Weitere Informationen finden Sie im <i>Informatica Big Data Management-Cluster-Integrationshandbuch</i>.</p>

## Eigenschaften zum Ausführen von Mappings im Hadoop-Cluster

Die folgende Tabelle beschreibt die erforderlichen Optionen für infacmd isp CreateConnection- und UpdateConnection-Befehle, die Sie konfigurieren, wenn Sie die Hive-Verbindung zum Ausführen von Informatica-Mappings im Hadoop-Cluster verwenden möchten:

Eigenschaft	Beschreibung
databaseName	Namespace für Tabellen. Verwenden Sie den Namen <code>default</code> für Tabellen, bei denen kein Datenbankname angegeben wurde.
customProperties	<p>Konfiguriert oder überschreibt Hive- oder Hadoop-Cluster-Eigenschaften in der <code>hive-site.xml</code>-Konfiguration auf dem Computer, auf dem der Datenintegrationsdienst ausgeführt wird. Sie können mehrere Eigenschaften angeben.</p> <p>Wählen Sie <b>Bearbeiten</b> aus, um den Namen und den Wert für die Eigenschaft anzugeben. Die Eigenschaft wird im folgenden Format angezeigt:</p> <pre>&lt;property1&gt;=&lt;value&gt;</pre> <p>Wenn Sie mehrere Eigenschaften angeben, wird <code>&amp;</code> als Trennzeichen für die Eigenschaften angezeigt.</p> <p>Die maximale Länge für das Format ist 1 MB.</p> <p>Wenn Sie eine erforderliche Eigenschaft für eine Hive-Verbindung eingeben, überschreibt diese die Eigenschaft, die Sie in den erweiterten Hive- bzw. Hadoop-Eigenschaften konfigurieren.</p> <p>Der Datenintegrationsdienst fügt diese Eigenschaften für jeden map-reduce-Job hinzu bzw. legt diese fest. Sie können diese Eigenschaften in der JobConf jedes mapper- oder reducer-Jobs überprüfen. Greifen Sie auf die JobConf jedes Jobs über die Jobtracker-URL unter jedem map-reduce-Job zu.</p> <p>Der Datenintegrationsdienst schreibt Meldungen für diese Eigenschaften in die Datenintegrationsdienst-Protokolle. Die Protokoll-Tracingebene im Datenintegrationsdienst muss so eingestellt sein, dass jede Zeile protokolliert wird. Alternativ dazu kann Verbose-Initialisierungstracing als Protokoll-Tracingebene eingestellt sein.</p> <p>Geben Sie zum Beispiel die folgenden Eigenschaften an, um die Anzahl der reducer-Jobs zur Ausführung eines mapping-Jobs zu begrenzen:</p> <pre>mapred.reduce.tasks=2&amp;hive.exec.reducers.max=10</pre>
stgDataCompressionCodecClass	Codec-Klassenname, der Datenkomprimierung ermöglicht und die Leistung in temporären Staging-Tabellen verbessert. Der Codec-Klassenname entspricht dem Code-Typ.
stgDataCompressionCodecType	<p>Hadoop-Komprimierungsbibliothek für einen Komprimierungs-Codec-Klassennamen.</p> <p>Sie können „Keine“, „Zlib“, „Gzip“, „Snappy“, „Bz2“, „LZO“ oder „Benutzerdefiniert“ auswählen.</p> <p>Standardwert ist „Keine“.</p>

## IBM DB2-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer IBM DB2-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die IBM DB2-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
PassThruEnabled	Optional. Aktiviert Pass-Through-Sicherheit für die Verbindung. Wenn Sie Pass-Through-Sicherheit für eine Verbindung aktivieren, verwendet die Domäne nicht die im Verbindungsobjekt definierten Anmeldeinformationen, sondern den Benutzernamen und das Passwort des Clients, um sich an der entsprechenden Datenbank anzumelden.
MetadataAccessConnect String	<p>Erforderlich. JDBC-Verbindungs-URL für den Zugriff auf Metadaten in der Datenbank.</p> <pre>jdbc:informatica:db2:// &lt;Hostname&gt;:&lt;Port&gt;;DatabaseName=&lt;Datenbankname&gt;</pre> <p>Beim Importieren einer Tabelle aus dem Developer Tool oder dem Analyst Tool werden standardmäßig alle Tabellen unterhalb des standardmäßigen Schemanamens angezeigt. Um Tabellen unterhalb eines bestimmten Schemas anstelle des Standardschemas anzuzeigen, können Sie den Namen des Schemas angeben, aus dem Sie die Tabelle importieren möchten. Schließen Sie den Parameter „ischemaname“ in die URL ein, um den Schemanamen anzugeben. Beispiel: Mit der folgenden Syntax wird eine Tabelle aus einem bestimmten Schema importiert:</p> <pre>jdbc:informatica:db2:// &lt;Hostname&gt;:&lt;Port&gt;;DatabaseName=&lt;Datenbankname&gt;;ischemaname=&lt;Schema_Name&gt;</pre> <p>Um eine Tabelle in mehreren Schemas zu suchen und zu importieren, können Sie die Namen mehrerer Schemas im Parameter „ischemaname“ festlegen. Beim Namen eines Schemas wird die Groß-/Kleinschreibung beachtet. Wenn Sie mehrere Schemanamen angeben, können Sie keine Sonderzeichen verwenden. Trennen Sie Schemanamen durch senkrechte Striche ( ) voneinander. Beispiel: Mit der folgenden Syntax können Sie eine Tabelle in drei Schemas suchen und importieren:</p> <pre>jdbc:informatica:db2:// &lt;Hostname&gt;:&lt;Port&gt;;DatabaseName=&lt;Datenbankname&gt;;ischemaname=&lt;schema_name1&gt; &lt;schema_name2&gt; &lt;schema_name3&gt;</pre>

Option	Beschreibung
AdvancedJDBCSecurityOptions	<p>Optional. Datenbankparameter für Metadata-Zugriff auf eine sichere Datenbank. Informatica behandelt den Wert des Felds „AdvancedJDBCSecurityOptions“ als vertrauliche Daten und verschlüsselt die Parameter-Zeichenfolge.</p> <p>Um eine Verbindung zu einer sicheren Datenbank herzustellen, beziehen Sie die folgenden Parameter mit ein:</p> <ul style="list-style-type: none"> <li>- EncryptionMethod. Erforderlich. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf SSL festgelegt werden.</li> <li>- ValidateServerCertificate. Optional. Gibt an, ob Informatica das Zertifikat validiert, das vom Datenbankserver gesendet wird.</li> </ul> <p>Wenn dieser Parameter auf TRUE festgelegt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den HostNameInCertificate-Parameter angeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat.</p> <p>Wenn dieser Parameter auf "false" festgelegt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben.</p> <ul style="list-style-type: none"> <li>- HostNameInCertificate. Optional. Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, validiert Informatica den Hostnamen in der Verbindungszeichenfolge mit dem Hostnamen im SSL-Zertifikat.</li> <li>- TrustStore. Erforderlich. Pfad und Dateiname der Truststore-Datei, die das SSL-Zertifikat für die Datenbank enthält.</li> <li>- TrustStorePassword Erforderlich. Passwort der Truststore-Datei für die sichere Datenbank.</li> </ul> <p><b>Hinweis:</b> Eine vollständige Liste der sicheren JDBC-Parameter finden Sie in der DataDirect JDBC-Dokumentation.</p> <p>Informatica hängt die sichere JDBC-Parameter an die Verbindungszeichenfolge an. Wenn Sie die sicheren JDBC-Parameter direkt in den Verbindungsstring mit einbeziehen, geben Sie keine Parameter in das Feld „AdvancedJDBCSecurityOptions“ ein.</p>
DataAccessConnectionString	<p>Verbindungszeichenfolge für den Zugriff auf Daten in der Datenbank</p> <p>Geben Sie die Verbindungszeichenfolge im folgenden Format ein:</p> <p>&lt;Datenbankname&gt;</p>
CodePage	<p>Erforderlich. Codepage, die zum Lesen aus einer Quell-Datenbank oder zum Schreiben in eine Target-Datenbank verwendet wird.</p>
EnvironmentSQL	<p>Optional. SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt.</p> <p>Beispiel: ALTER SESSION SET CURRENT_SCHEMA=INFA_USR;</p> <p><b>Hinweis:</b> Setzen Sie Sonderzeichen in doppelte Anführungszeichen.</p>
TransactionSQL	<p>Optional. SQL-Befehle zum Ausführen vor jeder Transaktion. Der Datenintegrationsdienst führt die Transaktions-SQL am Anfang jeder Transaktion aus.</p> <p>Beispiel: SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;</p> <p><b>Hinweis:</b> Setzen Sie Sonderzeichen in doppelte Anführungszeichen.</p>
Tablespace	<p>Optional. Der Tablespace-Name der Datenbank.</p>

Option	Beschreibung
QuoteChar	Optional. Das Zeichen, das als Anführungszeichen in dieser Verbindung verwendet wird. Der Zeichentyp, der zur Kennzeichnung von Sonderzeichen und reservierten SQL-Schlüsselwörtern, wie WHERE, verwendet wird. Der Datenintegrationsdienst schließt mit dem ausgewählten Zeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Der Datenintegrationsdienst verwendet dieses Zeichen auch für die Eigenschaft „QuoteChar“. Standardwert ist 0.
EnableQuotes	Optional. Kann zum Aktivieren von Anführungszeichen für diese Verbindung gewählt werden. Sofern aktiviert, schließt der Datenintegrationsdienst Tabellen-, Ansichts-, Schema-, Synonym- und Spaltennamen in Bezeichnerzeichen ein, wenn SQL für diese Objekte in der Verbindung erzeugt und ausgeführt wird. Zu verwenden, wenn Objekte Namen mit gemischter Groß-/Kleinschreibung oder kleingeschriebene Namen haben. Gültige Werte sind „True“ oder „False“. Standardwert ist „True“.
EnableConnectionPool	Optional. Aktiviert das Verbindungspooling. Wenn Sie Verbindungspooling aktivieren, behält der Verbindungspool inaktive Verbindungsinstanzen im Speicher. Wenn Sie Verbindungspooling deaktivieren, stoppt der Datenintegrationsdienst alle Poolingaktivitäten. Gültige Werte sind „True“ oder „False“. Standardwert ist „True“.
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Datenintegrationsdienst für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Standardwert ist 15.
ConnectionPoolMaxIdleTime	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird. Standardwert ist 120.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Standardwert ist 0.

## IMS-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer IMS-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die IMS-Verbindungsoptionen beschrieben:

Option	Beschreibung
CodePage	Erforderlich. Code zum Lesen aus oder Schreiben in die Datenbank. Verwenden Sie den ISO-Codepage-Namen, z. B. ISO-8859-6. Der Codepage-Name berücksichtigt keine Groß- und Kleinschreibung.
ArraySize	Optional. Bestimmt die Anzahl der Datensätze im Speicher-Array für die Threads, wenn der Worker-Threads-Wert größer als 0 ist. Gültige Werte sind 1 bis 5000. Standardwert ist 25.
Komprimierung	Optional. Komprimiert die Daten, um die Menge an Daten zu reduzieren, die Informatica-Anwendungen über das Netzwerk schreiben. „True“ oder „False“. Standardwert ist „False“.
EncryptionLevel	Optional. Verschlüsselungsebene. Wenn Sie AES für die Option EncryptionType angeben, müssen Sie einen der folgenden Werte angeben, um die Ebene der AES-Verschlüsselung anzugeben: <ul style="list-style-type: none"> <li>- 1. Verwenden Sie einen 128-Bit-Verschlüsselungsschlüssel.</li> <li>- 2. Verwenden Sie einen 192-Bit-Verschlüsselungsschlüssel.</li> <li>- 3. Verwenden Sie einen 256-Bit-Verschlüsselungsschlüssel.</li> </ul> Standardwert ist 1. <b>Hinweis:</b> Wenn Sie für den Verschlüsselungstyp „Keine“ auswählen, ignoriert der Datenintegrationsdienst den Wert für die Verschlüsselungsebene.
EncryptionType	Optional. Steuert, ob Verschlüsselung verwendet werden soll. Geben Sie einen der folgenden Werte an: <ul style="list-style-type: none"> <li>- Keine</li> <li>- AES</li> </ul> Standardwert ist „Keine“.
InterpretAsRows	Optional. Bei TRUE gibt die Pacing-Größe eine Anzahl von Zeilen wieder. Bei „false“ gibt die Pacing-Größe Kilobyte wieder. Standardwert ist „false“.
Speicherort:	Speicherort des PowerExchange Listener-Knotens, der eine Verbindung zur Datenbank herstellen kann. Der Speicherort ist im ersten Parameter der NODE-Anweisung in der PowerExchange-Konfigurationsdatei „dbmover.cfg“ angegeben.
OffLoadProcessing	Optional. Verschiebt die Stapeldatenverarbeitung vom Quellcomputer zum Computer des Datenintegrationsdiensts. Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- Auto. Der Datenintegrationsdienst bestimmt, ob Offload-Verarbeitung verwendet werden soll.</li> <li>- Ja. Offload-Verarbeitung wird verwendet.</li> <li>- Nein. Offload-Verarbeitung wird nicht verwendet.</li> </ul> Standardwert ist „Auto“.
PacingSize	Optional. Verlangsamt die Datenübertragungsrate, um Engpässe zu reduzieren. Je geringer der Wert ist, desto höher ist die Sitzungsleistung. Der Mindestwert lautet 0. Geben Sie 0 für optimale Leistung ein. Standardwert ist 0.
WorkerThread	Optional. Anzahl der vom Datenintegrationsdienst verwendeten Threads, um Stapeldaten bei aktivierter Offload-Verarbeitung zu verarbeiten. Um eine optimale Leistung zu erzielen, sollte dieser Wert die Anzahl der verfügbaren Prozessoren auf dem Rechner des Datenintegrationsdienstes nicht überschreiten. Gültige Werte sind 1 bis 64. Standardwert ist 0, wodurch Multithreading deaktiviert wird.



Option	Beschreibung
WriteMode	Geben Sie einen der folgenden Schreibmodi ein: <ul style="list-style-type: none"> <li>- CONFIRMWRITEON. Sendet Daten zum PowerExchange Listener und wartet auf eine Erfolgs-/Nichterfolgsreaktion, bevor weitere Daten gesendet werden.</li> <li>- CONFIRMWRITEOFF. Sendet Daten zum PowerExchange Listener, ohne eine Erfolgs-/Nichterfolgsreaktion abzuwarten. Verwenden Sie diese Option, wenn die Target-Tabelle bei Auftreten eines Fehlers erneut geladen werden kann.</li> <li>- ASYNCHRONOUSWITHFAULTT. Sendet Daten asynchron zum PowerExchange Listener mit der Möglichkeit der Fehlererkennung.</li> </ul> Der Standardwert ist CONFIRMWRITEON.
EnableConnectionPool	Optional. Aktiviert das Verbindungspooling. Wenn Sie Verbindungspooling aktivieren, behält der Verbindungspool inaktive Verbindungsinstanzen im Speicher. Wenn Sie Verbindungspooling deaktivieren, stoppt der Datenintegrationsdienst alle Poolingaktivitäten. „True“ oder „False“. Standardwert ist „False“.
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Datenintegrationsdienst für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Standardwert ist 15.
ConnectionPoolMaxIdleTime	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird. Standardwert ist 120.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleich oder kleiner als diese ist. Standardwert ist 0.

## JDBC-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer JDBC-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die JDBC-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
JDBCDriverClassName	<p>Die Java-Klasse, die zum Herstellen einer Verbindung zur Datenbank verwendet wird. Die folgende Liste enthält den Treiberklassennamen, den Sie für den entsprechenden Datenbanktyp eingeben können:</p> <ul style="list-style-type: none"> <li>- DataDirect-JDBC-Treiberklassenname für Oracle: com.informatica.jdbc.oracle.OracleDriver</li> <li>- DataDirect-JDBC-Treiberklassenname für IBM DB2: com.informatica.jdbc.db2.DB2Driver</li> <li>- DataDirect-JDBC-Treiberklassenname für Microsoft SQL Server: com.informatica.jdbc.sqlserver.SQLServerDriver</li> <li>- DataDirect-JDBC-Treiberklassenname für Sybase ASE: com.informatica.jdbc.sybase.SybaseDriver</li> <li>- DataDirect-JDBC-Treiberklassenname für Informix: com.informatica.jdbc.informix.InformixDriver</li> <li>- DataDirect-JDBC-Treiberklassenname für MySQL: com.informatica.jdbc.mysql.MySQLDriver</li> </ul> <p>Weitere Informationen zu den mit bestimmten Datenbanken zu verwendenden Treiberklassen finden Sie in der Dokumentation des Herstellers.</p>
MetadataConnString	<p>Die URL, die zum Herstellen einer Verbindung zur Datenbank verwendet wird. Die folgende Liste enthält die Verbindungszeichenfolge, die Sie für den entsprechenden Datenbanktyp eingeben können:</p> <ul style="list-style-type: none"> <li>- DataDirect-JDBC-Treiber für Oracle: jdbc:informatica:oracle://&lt;hostname&gt;:&lt;port&gt;;SID=&lt;sid&gt;</li> <li>- DataDirect-JDBC-Treiber für IBM DB2: jdbc:informatica:db2://&lt;hostname&gt;:&lt;port&gt;;DatabaseName=&lt;database name&gt;</li> <li>- DataDirect-JDBC-Treiber für Microsoft SQL Server jdbc:informatica:sqlserver://&lt;host&gt;:&lt;port&gt;;DatabaseName=&lt;database name&gt;</li> <li>- DataDirect-JDBC-Treiber für Sybase ASE: jdbc:informatica:sybase://&lt;host&gt;:&lt;port&gt;;DatabaseName=&lt;database name&gt;</li> <li>- DataDirect-JDBC-Treiber für Informix: jdbc:informatica:informix://&lt;host&gt;:&lt;port&gt;;informixServer=&lt;informix server name&gt;;databaseName=&lt;dbName&gt;</li> <li>- DataDirect-JDBC-Treiber für MySQL: jdbc:informatica:mysql://&lt;host&gt;:&lt;port&gt;;DatabaseName=&lt;database name&gt;</li> </ul> <p>Weitere Informationen über die für bestimmte Datenbanken zu verwendende Verbindungszeichenfolge finden Sie in der Dokumentation zur URL-Syntax des Herstellers.</p>
EnvironmentSQL	<p>Optional. SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt.</p> <p>Beispiel: ALTER SESSION SET CURRENT SCHEMA=INFA_USR;  <b>Hinweis:</b> Schließen Sie Sonderzeichen in doppelte Anführungszeichen ein.</p>
TransactionSQL	<p>Optional. SQL-Befehle zum Ausführen vor jeder Transaktion. Der Datenintegrationsdienst führt die Transaktions-SQL am Anfang jeder Transaktion aus.</p> <p>Beispiel: SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;  <b>Hinweis:</b> Setzen Sie Sonderzeichen in doppelte Anführungszeichen.</p>

Option	Beschreibung
QuoteChar	Optional. Das Zeichen, das als Anführungszeichen in dieser Verbindung verwendet wird. Der Zeichentyp, der zur Kennzeichnung von Sonderzeichen und reservierten SQL-Schlüsselwörtern, wie WHERE, verwendet wird. Der Datenintegrationsdienst schließt mit dem ausgewählten Zeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Der Datenintegrationsdienst verwendet dieses Zeichen auch für die Eigenschaft „QuoteChar“. Der Standardwert lautet „DOUBLE_QUOTE“.
EnableQuotes	Optional. Kann zum Aktivieren von Anführungszeichen für diese Verbindung gewählt werden. Sofern aktiviert, schließt der Datenintegrationsdienst Tabellen-, Ansichts-, Schema-, Synonym- und Spaltennamen in Bezeichnerzeichen ein, wenn SQL für diese Objekte in der Verbindung erzeugt und ausgeführt wird. Zu verwenden, wenn Objekte Namen mit gemischter Groß-/Kleinschreibung oder kleingeschriebene Namen haben. Gültige Werte sind „True“ oder „False“. Standardwert ist „True“.
hadoopConnector	Erforderlich, wenn Sie Sqoop-Konnektivität für das Datenobjekt aktivieren möchten, das die JDBC-Verbindung verwendet. Der Datenintegrationsdienst führt das Mapping in der Hadoop-Laufzeitumgebung über Sqoop aus.  Sie können Sqoop-Konnektivität für relationale Datenobjekte, benutzerdefinierte Datenobjekte und logische Datenobjekte konfigurieren, die auf einer JDBC-fähigen Datenbank basieren.  Legen Sie den Wert auf <code>SQOOP_146</code> fest, um Sqoop-Konnektivität zu aktivieren.
hadoopConnectorArgs	Optional. Geben Sie die Argumente ein, die von Sqoop zum Herstellen einer Verbindung zur Datenbank verwendet werden müssen. Schließen Sie die Sqoop-Argumente in einfache Anführungszeichen ein. Trennen Sie mehrere Argumente durch ein Leerzeichen.  Beispiel: <code>hadoopConnectorArgs='--&lt;Sqoop-Argument 1&gt; --&lt;Sqoop-Argument 2&gt;'</code>  Zum Lesen von Daten aus bzw. Schreiben von Daten in Teradata über spezielle TDCH-Konnektoren (Teradata Connector for Hadoop) für Sqoop definieren Sie die Klasse der TDCH-Verbindungs-Factory im Argument „hadoopConnectorArgs“. Die Klasse der Verbindungs-Factory richtet sich nach dem TDCH-Sqoop-Konnektor, der verwendet werden soll. <ul style="list-style-type: none"> <li>- Zur Verwendung von Cloudera Connector Powered by Teradata konfigurieren Sie das Argument „hadoopConnectorArgs“ folgendermaßen:  <pre>hadoopConnectorArgs='- Dsqaop.connection.factories=com.cloudera.connector.teradata.Teradata ManagerFactory'</pre> </li> <li>- Zur Verwendung von Hortonworks Connector for Teradata (unterstützt von Teradata Connector for Hadoop) konfigurieren Sie das Argument „hadoopConnectorArgs argument“ folgendermaßen:  <pre>hadoopConnectorArgs='- Dsqaop.connection.factories=org.apache.sqoop.teradata.TeradataManage rFactory'</pre> </li> </ul> Wenn Sie keine Sqoop-Argumente eingeben, erstellt der Datenintegrationsdienst den Sqoop-Befehl basierend auf den JDBC-Verbindungseigenschaften.

## JDBC V2-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer JDBC V2-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Beispiel:

```
./infacmd.sh createConnection -dn Domain_irl63ppd06 -un Administrator -pd SAM123 -cn
PostgreSQL -cid PostgreSQL -ct JDBC_V2 -cun
```

```

adaptersX1 -cpd adaptersX1 -o "connectionstring=' jdbc:postgresql://aurapostgres-
appsk.c5wj9sntucrg.ap-south-1.rds.amazonaws.com:5432/
JDBCv2' jdbcdriverclassname='org.postgresql.Driver' schemaname='public'
subtype='PostgreSQL' supportmixedcaseidentifier='true'
quoteChar='(quotes)' "

```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die JDBC V2-Verbindungsoptionen für die Befehle „infacmd isp CreateConnection“ und „infacmd isp UpdateConnection“ beschrieben:

Option	Beschreibung
username	Der Datenbankbenutzername. Benutzername mit Zugriffsberechtigungen für Azure SQL Database, PostgreSQL oder eine relationale Datenbank.
password	Das Passwort für den Datenbankbenutzernamen.
schemaname	Der Schemaname für die Verbindung zur Datenbank
jdbcdriverclassname	Name der JDBC-Treiberklasse. Die folgende Liste enthält den Treiberklassennamen, den Sie für den entsprechenden Datenbanktyp eingeben können: <ul style="list-style-type: none"> <li>- JDBC-Treiberklassenname für die Azure SQL-Datenbank: com.microsoft.sqlserver.jdbc.SQLServerDriver</li> <li>- JDBC-Treiberklassenname für Aurora PostgreSQL: org.postgresql.Driver</li> </ul> Weitere Informationen zu den mit bestimmten Datenbanken zu verwendenden Treiberklassen finden Sie in der Dokumentation des Herstellers.
connectionstring	Verbindungszeichenfolge zur Anmeldung bei der Datenbank. Verwenden Sie die folgende Verbindungszeichenfolge: <pre>jdbc:&lt;subprotocol&gt;:&lt;subname&gt;</pre> Die folgende Liste enthält die Beispiels-Verbindungszeichenfolgen, die Sie für den entsprechenden Datenbanktyp eingeben können: <ul style="list-style-type: none"> <li>- Verbindungszeichenfolge für den JDBC-Treiber der Azure SQL-Datenbank: jdbc:informatica:oracle://&lt;host&gt;:&lt;port&gt;;SID=&lt;value&gt;</li> <li>- Verbindungszeichenfolge für den JDBC-Treiber von Aurora PostgreSQL: jdbc:postgresql://&lt;host&gt;:&lt;port&gt;[/dbname]</li> </ul> Weitere Informationen über die Verbindungszeichenfolge, die mit bestimmten Treibern verwendet werden soll, finden Sie in der Dokumentation des Anbieters.
subtype	Der Typ der Datenbank, zu der Sie eine Verbindung herstellen möchten. Sie können für die Verbindung aus den folgenden Datenbanktypen auswählen: <ul style="list-style-type: none"> <li>- <b>Azure SQL-Datenbank.</b> Stellt eine Verbindung zur Azure SQL-Datenbank her.</li> <li>- <b>PostgreSQL</b> Stellt eine Verbindung zur Aurora PostgreSQL-Datenbank her.</li> <li>- <b>Andere</b> Verbindet sich mit jeder Datenbank, die den JDBC-Treiber Typ 4 unterstützt.</li> </ul>

Option	Beschreibung
supportmixedcaseidentifier	<p>Aktivieren Sie diese Eigenschaft, wenn die Datenbank IDs für gemischte Groß-/Kleinschreibung verwendet. Bei aktivierter Eigenschaft schließt der Datenintegrationsdienst alle IDs innerhalb des Zeichens ein, das für die Eigenschaft <b>SQL-Kennungszeichen</b> ausgewählt wurde.</p> <p>Beispielsweise unterstützt die PostgreSQL-Datenbank die gemischte Groß-/Kleinschreibung. Sie müssen diese Eigenschaft aktivieren, um eine Verbindung zur PostgreSQL-Datenbank herzustellen.</p> <p>Wenn die Eigenschaft <b>SQL-Kennungszeichen</b> auf „Kein“ festgelegt ist, wird die Eigenschaft <b>Unterstützte IDs für gemischte Groß-/Kleinschreibung</b> deaktiviert.</p>
quoteChar	<p>Art des Zeichens, das von der Datenbank verwendet wird, um Delimiter-IDs in SQL-Abfragen einzuschließen. Die verfügbaren Zeichen richten sich nach dem Datenbanktyp.</p> <p>Wählen Sie (Keine) aus, wenn die Datenbank reguläre IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst IDs nicht in Delimiter-Zeichen ein.</p> <p>Wählen Sie ein Zeichen aus, wenn die Datenbank Delimiter-IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst Delimiter-IDs in dieses Zeichen ein.</p>

## JD Edwards EnterpriseOne-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer JD Edwards EnterpriseOne-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

... -o option\_name=value option\_name=value ...

Beispiel:

```
infacmd.bat createConnection -dn DomainName -un Domain_UserName -pd Domain_Pwd -cn
conName -cid
conID -ct JDEE1 -o userName=JDEE1_DB_UserName password=JDEE1_DB_Pwd
enterpriseServer=JDE_ServerName
enterprisePort=JDE_DB_Port environment=JDE_Environment role=role
JDBCUserName=JDEE1_DB_UserName
JDBCPassword=JDEE1_DB_Pwd JDBCConnectionSTRING='DB connection string'
JDBCDriverClassName='jdbc driver classname'
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Um einen Wert einzugeben, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Wert in Anführungszeichen.

In der folgenden Tabelle werden die obligatorischen Verbindungsoptionen für JD Edwards EnterpriseOne für die Befehle „infacmd isp CreateConnection“ und „infacmd isp UpdateConnection“ beschrieben:

Eigenschaft	Beschreibung
userName	JD Edwards EnterpriseOne-Benutzername.
password	Passwort für den JD Edwards EnterpriseOne-Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet.
enterpriseServer	Der Hostname des JD Edwards EnterpriseOne-Servers, auf den zugegriffen werden soll.
enterprisePort	Die Portnummer für den Zugriff auf den JD Edwards EnterpriseOne-Server.

Eigenschaft	Beschreibung
environment	Name der JD Edwards EnterpriseOne-Umgebung, zu der Sie eine Verbindung herstellen möchten.
role	Rolle des JD Edwards EnterpriseOne-Benutzers.

## Kafka-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Kafka-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Kafka-Verbindungsoptionen für die Befehle „infacmd isp CreateConnection“ und „UpdateConnection“ beschrieben:

Option	Beschreibung
connectionId	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
connectionType	Erforderlich. Verbindungstyp lautet KAFKA.
name	Erforderlich. Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * ( ) - + = { [ ]   \ : ; " ' < , > . ? /
connRetryTimeout	Anzahl der Sekunden, in denen der Integrationsdienst versucht, sich erneut mit dem Kafka-Broker zu verbinden. Ist die Quelle oder das Ziel für den angegebenen Zeitraum nicht verfügbar, wird die Zuordnungsausführung zur Vermeidung von Datenverlusten angehalten.
kafkaBrokerVersion	Die Version des Kafka-Messaging-Brokers. Sie können einen der folgenden Werte eingeben: - 0.10.1.x-2.0.0

Option	Beschreibung
kfkBrkList	<p>Die Kombination aus IP-Adresse und Port für die Broker-Liste des Kafka-Messaging-Systems. Die Kombination aus IP-Adresse und Port weist folgendes Format auf:</p> <pre>&lt;IP Address&gt;:&lt;port&gt;</pre> <p>Sie können mehrere kommasetrennte Kombinationen aus IP-Adresse und Port eingeben.</p>
zkHostPortList	<p>Die Kombination aus IP-Adresse und Port für Apache ZooKeeper zur Verwaltung der Konfiguration des Kafka-Messaging-Brokers. Die Kombination aus IP-Adresse und Port weist folgendes Format auf:</p> <pre>&lt;IP Address&gt;:&lt;port&gt;</pre> <p>Sie können mehrere kommasetrennte Kombinationen aus IP-Adresse und Port eingeben.</p>

## Kudu-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Kudu-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Kudu-Verbindungsoptionen für die Befehle `infacmd isp CreateConnection` und `UpdateConnection` beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf maximal 128 Zeichen umfassen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * ( ) - + = { [ ]   \ : ; " ' < , > . ? /
ID	<p>Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern.</p> <p>Als Standardwert dient der Verbindungsname.</p>
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie Kudu aus.

## LDAP-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer LDAP-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

... -o option\_name=value option\_name=value ...

Beispiel:

```
infacmd.sh createConnection -dn DomainName -un Domain_UserName -pd Domain_Pwd -cn  
conname -cid conname -ct ldap -o  
hostName=hostIPAddress port=port_number userName=ldapUserName password=LDAPPWD
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Um einen Wert einzugeben, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Wert in Anführungszeichen.

In der folgenden Tabelle werden die obligatorischen LDAP-Verbindungsoptionen für die Befehle „infacmd isp CreateConnection“ und „infacmd isp UpdateConnection“ beschrieben:

Eigenschaft	Beschreibung
hostName	Der Hostname des LDAP-Verzeichnisseservers, auf den zugegriffen werden soll.
port	Die Portnummer für den Zugriff auf den LDAP-Verzeichnisseserver.
userName	LDAP-Benutzername.
password	Passwort für den LDAP-Benutzernamen. Beim Passwort wird die Groß-/ Kleinschreibung beachtet.

## LinkedIn-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer LinkedIn-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

... -o option\_name=value option\_name=value ...

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die LinkedIn-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
ConsumerKey	Der API-Schlüssel, den Sie beim Erstellen der Anwendung in LinkedIn erhalten. LinkedIn verwendet den Schlüssel zur Identifizierung der Anwendung.
ConsumerSecret	Der Geheimschlüssel, den Sie beim Erstellen der Anwendung in LinkedIn erhalten. LinkedIn verwendet das Geheimwort für das Eigentum am Verbraucherschlüssel.



Option	Beschreibung
AccessToken	Zugriffstoken, den das OAuth-Dienstprogramm zurückgibt. Die LinkedIn-Anwendung verwendet diesen Token anstelle der Benutzeranmeldedaten für den Zugriff auf geschützte Ressourcen.
AccessSecret	Zugriffsgeheimwort, das das OAuth-Dienstprogramm zurückgibt. Das Geheimwort legt das Eigentum eines Token fest.

## MapR-DB Connection Options

Use connection options to define an HBase connection for MapR-DB.

Enter connection options in the following format:

... -o option\_name=value option\_name=value ...

To enter multiple options, separate them with a space. To enter a value that contains a space or non-alphanumeric character, enclose the value in quotation marks.

The following table describes the HBase connection options for MapR-DB for the `infacmd` `isp` `CreateConnection` and `UpdateConnection` commands:

Option	Description
DATABASETYPE	Required. Set the value to <code>MapR-DB</code> and enclose the value in single quotes.
clusterConfigId	The cluster configuration ID associated with the Hadoop cluster. You must enter a configuration ID to set up an HBase connection for MapR-DB.
maprdbpath	<p>Required. Set the value to the database path that contains the MapR-DB table that you want to connect to. Enter a valid MapR cluster path. Enclose the value in single quotes.</p> <p>When you create an HBase data object for MapR-DB, you can browse only tables that exist in the path that you specify in this option. You cannot access tables that are available in sub-directories in the specified path.</p> <p>For example, if you specify the <code>maprdbpath</code> as <code>/user/customers/</code>, you can access the tables in the <code>customers</code> directory. However, if the <code>customers</code> directory contains a sub-directory named <code>regions</code>, you cannot access the tables in the following directory:</p> <p><code>/user/customers/regions</code></p>

## Microsoft Azure Blob Storage-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Microsoft Azure Blob Storage-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

... -o option\_name=value option\_name=value ...

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder nicht-alphanumerisches Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Verbindungsoptionen von Azure Blob Storage für die Befehle „infacmd isp CreateConnection“ und „infacmd isp UpdateConnection“ beschrieben:

Option	Beschreibung
accountName	Name des Microsoft Azure Blob Storage-Kontos.
authenticationtype	Autorisierungstyp. Sie können einen der folgenden Autorisierungsmechanismen wählen: <ul style="list-style-type: none"> <li>- Shared-Key-Autorisierung</li> <li>- Signaturen für gemeinsamen Zugriff</li> </ul>
accountKey	Microsoft Azure Blob Storage-Zugriffsschlüssel.
sharedaccesssignature	Signaturen für gemeinsamen Zugriff. <b>Hinweis:</b> Selbst wenn Sie die Berechtigung für den gemeinsamen Zugriff nicht zum Erstellen einer Verbindung verwenden möchten, definieren Sie die Option in der Befehlszeile wie folgt: sharedaccesssignature=' '
containerName	Der Root-Container oder die Unterordner mit dem absoluten Pfad.
endpointSuffix	Typ der Microsoft Azure-Endpunkte. Sie können einen der folgenden Endpunkte angeben: <ul style="list-style-type: none"> <li>- core.windows.net: Standard</li> <li>- core.usgovcloudapi.net: Zum Auswählen der Microsoft Azure-Endpunkte (US-Regierung)</li> <li>- core.chinacloudapi.cn: Nicht anwendbar</li> </ul>

## Microsoft Azure Data Lake Storage Gen1-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Microsoft Azure Data Lake Storage Gen1-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

... -o option\_name=value option\_name=value ...

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder nicht-alphanumerisches Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden Verbindungsoptionen von Microsoft Azure Data Lake Storage Gen1 für die Befehle „infacmd isp CreateConnection“ und „infacmd isp UpdateConnection“ beschrieben:

Option	Beschreibung
ADLSAccountName	Microsoft Azure Data Lake Storage Gen1-Konto- oder Dienstname.
Client-ID	Die ID der Anwendung, in der die OAuth-Authentifizierung in Active Directory abgeschlossen werden soll.
Geheimer Clientschlüssel	Der geheime Schlüssel des Clients, mit dem die OAuth-Authentifizierung in Active Directory abgeschlossen werden soll.

Option	Beschreibung
Verzeichnis	Pfad eines vorhandenen Verzeichnisses auf dem angegebenen Dateisystem. Der Standardeinstellung ist das Root-Verzeichnis.
AuthEndpoint	Der Endpunkt des OAuth 2.0-Tokens, von dem aus Zugriffscodes basierend auf der Client-ID generiert wird und der geheime Client-Schlüssel fertiggestellt wird.

Weitere Informationen zum Erstellen einer Client-ID und eines Clientschlüssels erhalten Sie beim Azure-Administrator oder in der Dokumentation zu Microsoft Azure Data Lake Storage Gen1.

## Microsoft Azure Data Lake Storage Gen2-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Microsoft Azure Data Lake Storage Gen2-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

... -o option\_name=value option\_name=value ...

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder nicht-alphanumerisches Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden Verbindungsoptionen von Microsoft Azure Data Lake Storage Gen2 für die Befehle „`infacmd isp CreateConnection`“ und „`infacmd isp UpdateConnection`“ beschrieben:

Option	Beschreibung
accountName	Microsoft Azure Data Lake Storage Gen2-Konto- oder Dienstname.
Client-ID	Die ID der Anwendung, in der die OAuth-Authentifizierung in Active Directory abgeschlossen werden soll.
Geheimer Clientschlüssel	Der geheime Schlüssel des Clients, mit dem die OAuth-Authentifizierung in Active Directory abgeschlossen werden soll.
tenantID	Verzeichnis-ID des Azure Active Directory.
fileSystemName	Name eines vorhandenen Dateisystems in Microsoft Azure Data Lake Storage Gen2.
directoryPath	Pfad eines vorhandenen Verzeichnisses auf dem angegebenen Dateisystem. Der Standardeinstellung ist das Root-Verzeichnis.

Weitere Informationen zum Erstellen einer Client-ID, eines Clientschlüssels, einer Mandanten-ID und des Dateisystemnamens erhalten Sie beim Azure-Administrator oder in der Dokumentation zu Microsoft Azure Data Lake Storage Gen2.

## Microsoft Azure SQL Data Warehouse-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Microsoft Azure SQL Data Warehouse-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

... -o option\_name=value option\_name=value ...

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder nicht-alphanumerisches Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Verbindungsoptionen von Microsoft Azure SQL Data Warehouse für die Befehle „infacmd isp CreateConnection“ und „infacmd isp UpdateConnection“ beschrieben:

Option	Beschreibung
JdbcUrl	JDBC-Verbindungszeichenfolge von Microsoft Azure SQL Data Warehouse. Sie können beispielsweise folgende Verbindungszeichenfolge eingeben: jdbc:sqlserver://<Server>.database.windows.net:1433;database=<Datenbank>
JdbcUsername	Benutzername für die Verbindung zum Microsoft Azure SQL Data Warehouse-Konto.
JdbcPassword	Passwort für die Verbindung zum Microsoft Azure SQL Data Warehouse-Konto.
SchemaName	Name des Schemas in Microsoft Azure SQL Data Warehouse.
BlobAccountName	Name des Microsoft Azure Storage-Kontos zum Bereitstellen der Dateien.
BlobAccountKey	Microsoft Azure Storage-Zugriffsschlüssel zum Bereitstellen der Dateien.
EndPointSuffix	Typ der Microsoft Azure-Endpunkte. Sie können einen der folgenden Endpunkte angeben: - core.windows.net: Standard - core.usgovcloudapi.net: Zum Auswählen der Microsoft Azure-Endpunkte (US-Regierung) - core.chinacloudapi.cn: Nicht anwendbar
VNetRule	Aktivieren, um eine Verbindung zu einem Microsoft Azure SQL Data Warehouse-Endpunkt herzustellen, der sich in einem virtuellen Netzwerk (VNet) befindet.

## Microsoft SQL Server-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Microsoft SQL Server-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden Verbindungsoptionen von Microsoft SQL Server für die Befehle „infacmd isp CreateConnection“ und „UpdateConnection“ beschrieben:

Option	Beschreibung
UseTrustedConnection	Optional. Der Integrationsdienst verwendet die Windows-Authentifizierung, um auf die Microsoft SQL Server-Datenbank zuzugreifen. Der Name des Benutzers, der den Integrationsdienst startet, muss ein gültiger Windows-Benutzer mit Zugriff auf die Microsoft SQL Server-Datenbank sein. „True“ oder „False“. Standardwert ist FALSE.
PassThruEnabled	Optional. Aktiviert Pass-Through-Sicherheit für die Verbindung. Wenn Sie Pass-Through-Sicherheit für eine Verbindung aktivieren, verwendet die Domäne nicht die im Verbindungsobjekt definierten Anmeldeinformationen, sondern den Benutzernamen und das Passwort des Clients, um sich an der entsprechenden Datenbank anzumelden.

Option	Beschreibung
MetadataAccessConnectionString	<p>JDBC-Verbindungs-URL für den Zugriff auf Metadaten in der Datenbank.</p> <p>Verwenden Sie die folgende Verbindungs-URL:</p> <pre>jdbc:informatica:sqlserver:// &lt;Hostname&gt;:&lt;Port&gt;;DatabaseName=&lt;Datenbankname&gt;</pre> <p>Beziehen Sie zum Testen der Verbindung mit NTLM-Authentifizierung die folgenden Parameter in die Verbindungszeichenfolge ein:</p> <ul style="list-style-type: none"> <li>- AuthenticationMethod. Die zu verwendende Version der NTLM-Authentifizierung.</li> </ul> <p><b>Hinweis:</b> UNIX unterstützt NTLMv1 und NTLMv2, jedoch nicht NTLM.</p> <ul style="list-style-type: none"> <li>- Domäne. Die Domäne, zu der der SQL Server gehört.</li> </ul> <p>Das folgende Beispiel zeigt die Verbindungszeichenfolge für einen SQL Server, der NTLMv2-Authentifizierung in einer NT-Domäne namens „Informatica.com“ verwendet:</p> <pre>jdbc:informatica:sqlserver:// host01:1433;DatabaseName=SQL1;AuthenticationMethod=ntlm2java;Domain=Informatica.com</pre> <p>Wenn Sie eine Verbindung über NTLM-Authentifizierung herstellen, können Sie in den MS SQL Server-Verbindungseigenschaften die Option <b>Verwenden Sie trusted Verbindung</b> aktivieren. Wenn Sie eine Verbindung über NTLMv1- oder NTLMv2-Authentifizierung herstellen, müssen Sie den Benutzernamen und das Kennwort in den Verbindungseigenschaften angeben.</p>
AdvancedJDBCSecurityOptions	<p>Optional. Datenbankparameter für Metadata-Zugriff auf eine sichere Datenbank. Informatica behandelt den Wert des Felds „AdvancedJDBCSecurityOptions“ als vertrauliche Daten und verschlüsselt die Parameter-Zeichenfolge.</p> <p>Um eine Verbindung zu einer sicheren Datenbank herzustellen, beziehen Sie die folgenden Parameter mit ein:</p> <ul style="list-style-type: none"> <li>- EncryptionMethod. Erforderlich. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf SSL festgelegt werden.</li> <li>- ValidateServerCertificate. Optional. Gibt an, ob Informatica das Zertifikat validiert, das vom Datenbankserver gesendet wird.</li> </ul> <p>Wenn dieser Parameter auf TRUE festgelegt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den HostNameInCertificate-Parameter angeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat.</p> <p>Wenn dieser Parameter auf "false" festgelegt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben.</p> <ul style="list-style-type: none"> <li>- HostNameInCertificate. Optional. Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, validiert Informatica den Hostnamen in der Verbindungszeichenfolge mit dem Hostnamen im SSL-Zertifikat.</li> <li>- TrustStore. Erforderlich. Pfad und Dateiname der Truststore-Datei, die das SSL-Zertifikat für die Datenbank enthält.</li> <li>- TrustStorePassword. Erforderlich. Passwort der Truststore-Datei für die sichere Datenbank.</li> </ul> <p><b>Hinweis:</b> Eine vollständige Liste der sicheren JDBC-Parameter finden Sie in der DataDirect JDBC-Dokumentation.</p> <p>Informatica hängt die sicheren JDBC-Parameter an die Verbindungszeichenfolge an. Wenn Sie die sicheren JDBC-Parameter direkt in der Verbindungszeichenfolge einschließen, geben Sie keinen Parameter in das Feld AdvancedJDBCSecurityOptions ein.</p>
DataAccessConnectionString	<p>Erforderlich. Verbindungszeichenfolge für den Zugriff auf Daten in der Datenbank</p> <p>Geben Sie die Verbindungszeichenfolge im folgenden Format ein:</p> <pre>&lt;Servername&gt;@&lt;Datenbankname&gt;</pre>

Option	Beschreibung
DomainName	Optional. Der Name der Domäne, in der Microsoft SQL Server ausgeführt wird.
PacketSize	Optional. Erhöhen Sie die Netzwerkpaketgröße, damit größere Datenpakete das Netzwerk gleichzeitig durchlaufen können.
CodePage	Erforderlich. Code zum Lesen aus oder Schreiben in die Datenbank. Verwenden Sie den ISO-Codepage-Namen, z. B. ISO-8859-6. Der Codepage-Name berücksichtigt keine Groß- und Kleinschreibung.
UseDSN	Erforderlich. Legt fest, ob der Datenintegrationsdienst den Namen der Datenquelle für die Verbindung verwenden muss. Wenn Sie den Optionswert auf „true“ festlegen, ruft der Datenintegrationsdienst den Datenbanknamen und den Servernamen aus dem DSN ab. Wenn Sie den Optionswert auf „true“ festlegen, müssen Sie den Datenbanknamen und den Servernamen eingeben.
ProviderType	Erforderlich. Der Verbindungsprovider, den Sie für eine Verbindung zur Microsoft SQL-Serverdatenbank nutzen möchten. Sie können einen der folgenden Werte definieren: <ul style="list-style-type: none"> <li>- 0. Legen Sie den Wert auf 0 fest, wenn Sie den ODBC-Providertyp verwenden möchten. Standardwert ist 0.</li> <li>- 1. Legen Sie den Wert auf 1 fest, wenn Sie den OLEDB-Providertyp verwenden möchten.</li> </ul>
OwnerName	Optional. Der Name des Tabelleneigentümers.
SchemaName	Optional. Der Name des Schemas in der Datenbank. Sie müssen den Schemanamen für das Profiling-Warehouse angeben, wenn der Schemaname anders lautet als der Benutzername für die Datenbank. Sie müssen den Schemanamen für die Datenobjekt-Cache-Datenbank angeben, wenn der Schemaname nicht mit dem Datenbank-Benutzernamen übereinstimmt und Sie benutzerverwaltete Cache-Tabellen konfigurieren.
EnvironmentSQL	Optional. SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt. <b>Beispiel:</b> ALTER SESSION SET CURRENT_SCHEMA=INFA_USR; <b>Hinweis:</b> Setzen Sie Sonderzeichen in doppelte Anführungszeichen.
TransactionSQL	Optional. SQL-Befehle zum Ausführen vor jeder Transaktion. Der Datenintegrationsdienst führt die Transaktions-SQL am Anfang jeder Transaktion aus. <b>Beispiel:</b> SET TRANSACTION ISOLATION LEVEL SERIALIZABLE; <b>Hinweis:</b> Setzen Sie Sonderzeichen in doppelte Anführungszeichen.
QuoteChar	Optional. Das Zeichen, das als Anführungszeichen in dieser Verbindung verwendet wird. Der Zeichentyp, der zur Kennzeichnung von Sonderzeichen und reservierten SQL-Schlüsselwörtern, wie WHERE, verwendet wird. Der Datenintegrationsdienst schließt mit dem ausgewählten Zeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Der Datenintegrationsdienst verwendet dieses Zeichen auch für die Eigenschaft „QuoteChar“. Standardwert ist 0.

Option	Beschreibung
EnableQuotes	Optional. Wählen Sie diesen Wert, um Anführungszeichen für diese Verbindung zu aktivieren.  Sofern aktiviert, schließt der Datenintegrationsdienst Tabellen-, Ansichts-, Schema-, Synonym- und Spaltennamen in Bezeichnerzeichen ein, wenn SQL für diese Objekte in der Verbindung erzeugt und ausgeführt wird. Zu verwenden, wenn Objekte Namen mit gemischter Groß-/Kleinschreibung oder kleingeschriebene Namen haben. Gültige Werte sind „True“ oder „False“. Standardwert ist „True“.
EnableConnectionPool	Optional. Aktiviert das Verbindungspooling. Wenn Sie Verbindungspooling aktivieren, behält der Verbindungspool inaktive Verbindungsinstanzen im Speicher. Wenn Sie Verbindungspooling deaktivieren, stoppt der Datenintegrationsdienst alle Poolingaktivitäten. Gültige Werte sind „True“ oder „False“. Standardwert ist „True“.
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Datenintegrationsdienst für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Standardwert ist 15.
ConnectionPoolMaxIdleTime	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird. Standardwert ist 120.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Standardwert ist 0.

## Microsoft Dynamics CRM-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Microsoft Dynamics CRM-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Beispiel:

```
./infacmd.sh createconnection -dn Domain_Adapters_1020_Uni -un Administrator -pd
Administrator -cn msd_cmdline AD -cid msd_cmdline_edit -ct MSDYNAMICS -o
"AuthenticationType=Passport DiscoveryServiceURL=https://disco.crm8.dynamics.com/
XRMServices/2011/Discovery.svc Username=skmanja@InformaticaLLC.onmicrosoft.com
Password=AwesomeDay103 OrganizationName=org00faf3b6 Domain=<dummy value>
SECURITYTOKENSERVICE=<dummy value>"
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden Verbindungsoptionen von Microsoft Dynamics CRM für die Befehle „infacmd isp CreateConnection“ und „infacmd isp UpdateConnection“ beschrieben:

Option	Beschreibung
AuthenticationType	<p>Erforderlich. Authentifizierungstyp für die Verbindung. Geben Sie einen der folgenden Authentifizierungstypen an:</p> <ul style="list-style-type: none"> <li>- „Passport“. Wird häufig für die Online-Bereitstellung und für die Kombination von Online-Bereitstellung und Bereitstellung mit Internetzugriff von Microsoft Dynamics CRM verwendet.</li> <li>- „Claims-based“. Wird häufig für die lokale Bereitstellung und die Bereitstellung mit Internetzugriff von Microsoft Dynamics CRM verwendet.</li> <li>- „Active directory“. Wird häufig für die lokale Bereitstellung von Microsoft Dynamics CRM verwendet.</li> </ul>
DiscoveryServiceURL	<p>Erforderlich. URL des Microsoft Dynamics CRM-Diensts.</p> <p>Verwenden Sie das folgende Format: &lt;http/https&gt;://&lt;Name des Anwendungsservers&gt;:&lt;Port&gt;/XRMService/2011/Discovery.svc</p> <p>Um die Ermittlungsdienst-URL zu suchen, melden Sie sich bei der Microsoft Live-Instanz an und klicken Sie auf <b>Einstellungen &gt; Anpassung &gt; Entwicklerressourcen</b>.</p>
Domain	<p>Erforderlich. Domäne, zu der der Benutzer gehört. Sie müssen den vollständigen Domänennamen angeben. Beispiel: msd.sampledomain.com.</p> <p>Konfigurieren Sie die Domäne für die Active Directory-Authentifizierung und die anspruchsbasierte Authentifizierung.</p> <p><b>Hinweis:</b> Wenn Sie den Authentifizierungstyp „Passport“ auswählen, müssen Sie einen Dummy-Wert für „Domain“ bereitstellen.</p>
ConfigFilesForMetadata	<p>Konfigurationsverzeichnis für den Client.</p> <p>Standardverzeichnis ist: &lt;INFA_HOME&gt;/clients/DeveloperClient/msdcrm/conf</p>
OrganizationName	<p>Erforderlich. Microsoft Dynamics CRM-Organisationsname. Bei Organisationsnamen wird zwischen Groß- und Kleinschreibung unterschieden.</p> <p>Verwenden Sie für die Microsoft Live-Authentifizierung den eindeutigen Namen der Organisation in Microsoft Live.</p> <p>Um den eindeutigen Namen der Organisation zu suchen, melden Sie sich bei der Microsoft Live-Instanz an und klicken Sie auf <b>Einstellungen &gt; Anpassung &gt; Entwicklerressourcen</b>.</p>
Passwort	Erforderlich. Passwort zum Authentifizieren des Benutzers.
ConfigFilesForData	<p>Konfigurationsverzeichnis für den Server.</p> <p>Wenn sich die Server-Datei in einem anderen Verzeichnis befindet, geben Sie den Verzeichnispfad an.</p>
SecurityTokenService	<p>Erforderlich. URL des Microsoft Dynamics CRM-Sicherheits-Token-Diensts.</p> <p>Beispiel: https://sts1.&lt;Unternehmen&gt;.com.</p> <p>Nehmen Sie die Konfiguration für die anspruchsbasierte Authentifizierung vor.</p> <p><b>Hinweis:</b> Wenn Sie den Authentifizierungstyp „Passport“ oder „Active Directory“ auswählen, müssen Sie einen Dummy-Wert für SecurityTokenService bereitstellen.</p>
Benutzername	Erforderlich. Benutzer-ID, die bei Microsoft Dynamics CRM registriert ist.



Option	Beschreibung
UseMetadataConfigForDataAccess	Wählen Sie diese Option aus, wenn sich die Konfigurationsdatei und die Serverdatei im selben Verzeichnis befinden.  Falls sich die Serverdatei in einem anderen Verzeichnis befindet, deaktivieren Sie diese Option und geben Sie im Feld „Datenzugriff“ den Verzeichnispfad an. Geben Sie einen der folgenden Werte an: - „true“ für aktiviert - „false“ für nicht aktiviert
KeyStoreFileName	Enthält die für die sichere Kommunikation erforderlichen Schlüssel und Zertifikate.  Wenn Sie die Java-cacerts-Datei verwenden möchten, löschen Sie den Inhalt dieses Felds.
KeyStorePassword	Passwort für die Datei <code>infa_keystore.jks</code> .  Wenn Sie die Java-cacerts-Datei verwenden möchten, löschen Sie den Inhalt dieses Felds.
TrustStoreFileName	Legen Sie <code>INFA_TRUSTSTORE</code> in den Umgebungsvariablen fest. Das Verzeichnis muss die <code>truststore</code> -Datei <code>infa_truststore.jks</code> enthalten. Falls die Datei nicht im angegebenen Pfad verfügbar ist, prüft der Datenintegrationsdienst das Zertifikat in der Java-cacerts-Datei.  Wenn Sie die Java-cacerts-Datei verwenden möchten, löschen Sie den Inhalt dieses Felds.
TrustStorePassword	Passwort für die Datei <code>infa_keystore.jks</code> .  Wenn Sie die Java-cacerts-Datei verwenden möchten, löschen Sie den Inhalt dieses Felds.

## Netezza-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Netezza-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

... -o option\_name=value option\_name=value ...

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Netezza-Verbindungsoptionen für die `infacmd` `isp` `CreateConnection`- und `UpdateConnection`-Befehle beschrieben:

Option	Beschreibung
connectionString	Erforderlich. Name der ODBC-Datenquelle, die Sie zum Herstellen einer Verbindung zur Netezza-Datenbank erstellen.
jdbcUrl	Erforderlich. JDBC-URL, die vom Developer Tool beim Herstellen einer Verbindung zur Netezza-Datenbank verwendet werden muss. Verwenden Sie das folgende Format: <code>jdbc:netezza://&lt;hostname&gt;:&lt;port&gt;/&lt;database name&gt;</code>
username	Erforderlich. Benutzername mit den entsprechenden Berechtigungen für den Zugriff auf die Netezza-Datenbank.

Option	Beschreibung
password	Erforderlich. Passwort für den Datenbankbenutzernamen.
timeout	Erforderlich. Zeit in Sekunden, die das Developer Tool auf eine Antwort von der Netezza-Datenbank wartet, ehe es die Verbindung schließt.

## OData-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer OData-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die OData-Verbindungsoptionen für die `infacmd isp CreateConnection-` und `UpdateConnection-`Befehle beschrieben:

Eigenschaft	Beschreibung
URL	Erforderlich. Root-URL des OData-Diensts, die die Daten bereitstellt, die Sie lesen möchten.
securityType	Optional. Sicherheitsprotokoll, das das Developer Tool verwenden muss, um eine sichere Verbindung mit dem OData-Server herzustellen. Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- Keiner</li> <li>- SSL</li> <li>- TLS</li> </ul>
trustStoreFileName	Erforderlich, wenn Sie einen Sicherheitstyp eingeben. Name der Truststore-Datei, die das öffentliche Zertifikat für den OData-Server enthält.
trustStorePassword	Erforderlich, wenn Sie einen Sicherheitstyp eingeben. Passwort für die Truststore-Datei, die das öffentliche Zertifikat für den OData-Server enthält.
keyStoreFileName	Erforderlich, wenn Sie einen Sicherheitstyp eingeben. Name der Schlüsselspeicherdatei, die den privaten Schlüssel für den OData-Server enthält.
keyStorePassword	Erforderlich, wenn Sie einen Sicherheitstyp eingeben. Passwort für die Schlüsselspeicherdatei, die den privaten Schlüssel für den OData-Server enthält.

## ODBC-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer ODBC-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die ODBC-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
PassThruEnabled	Optional. Aktiviert Pass-Through-Sicherheit für die Verbindung. Wenn Sie Pass-Through-Sicherheit für eine Verbindung aktivieren, verwendet die Domäne nicht die im Verbindungsobjekt definierten Anmeldeinformationen, sondern den Benutzernamen und das Passwort des Clients, um sich an der entsprechenden Datenbank anzumelden.
DataAccessConnectString	Verbindungsstring für den Zugriff auf Daten in der Datenbank. Geben Sie den Verbindungsstring im folgenden Format ein: <Datenbankname>
CodePage	Erforderlich. Codepage, die zum Lesen aus einer Quell-Datenbank oder zum Schreiben auf eine Target-Datenbank oder -Datei verwendet wird.
EnvironmentSQL	Optional. SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt. <b>Beispiel:</b> ALTER SESSION SET CURRENT_SCHEMA=INFA_USR; <b>Hinweis:</b> Setzen Sie Sonderzeichen in doppelte Anführungszeichen.
TransactionSQL	Optional. SQL-Befehle zum Ausführen vor jeder Transaktion. Der Datenintegrationsdienst führt die Transaktions-SQL am Anfang jeder Transaktion aus. <b>Beispiel:</b> SET TRANSACTION ISOLATION LEVEL SERIALIZABLE; <b>Hinweis:</b> Setzen Sie Sonderzeichen in doppelte Anführungszeichen.
QuoteChar	Optional. Das Zeichen, das als Anführungszeichen in dieser Verbindung verwendet wird. Der Zeichentyp, der verwendet wird, um Sonderzeichen und reservierte SQL-Schlüsselwörter wie WHERE zu kennzeichnen. Der Datenintegrationsdienst schließt mit dem ausgewählten Zeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Der Datenintegrationsdienst verwendet dieses Zeichen auch für die Eigenschaft „QuoteChar“. Der Standardwert ist 4.
ODBC-Provider	Optional. Der Datenbanktyp, zu dem der Datenintegrationsdienst mit ODBC eine Verbindung herstellt. Geben Sie zur Pushdown-Optimierung den Datenbanktyp an, damit der Datenintegrationsdienst die native Datenbank-SQL generieren kann. Es gibt die folgenden Optionen: - Andere - Sybase - Microsoft_SQL_Server - Teradata - Netezza - Greenplum Standardwert ist „Andere“.

Option	Beschreibung
EnableQuotes	Optional. Wählen Sie diesen Wert, um Anführungszeichen für diese Verbindung zu aktivieren.  Sofern aktiviert, umgibt der Datenintegrationsdienst Tabellen-, Ansichts-, Schema-, Synonym- und Spaltennamen beim Generieren und Ausführen von SQL für diese Objekte in der Verbindung mit ID-Zeichen. Zu verwenden, wenn Objekte Namen mit gemischter Groß-/Kleinschreibung oder kleingeschriebene Namen haben. Gültige Werte sind „true“ oder „false“. Standardwert ist „false“.
EnableConnectionPool	Optional. Ermöglicht das Verbindungspooling. Wenn Sie Verbindungspooling aktivieren, behält der Verbindungspool inaktive Verbindungsinstanzen im Speicher. Wenn Sie Verbindungspooling deaktivieren, stoppt der Datenintegrationsdienst alle Poolingaktivitäten. Gültige Werte sind „true“ oder „false“. Standardwert ist „true“.
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Datenintegrationsdienst für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Standardwert ist 15.
ConnectionPoolMaxIdleTime	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird. Standardwert ist 120.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Standardwert ist 0.

## Oracle-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Oracle-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Oracle-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
PassThruEnabled	Optional. Aktiviert Pass-Through-Sicherheit für die Verbindung. Wenn Sie Pass-Through-Sicherheit für eine Verbindung aktivieren, verwendet die Domäne nicht die im Verbindungsobjekt definierten Anmeldeinformationen, sondern den Benutzernamen und das Passwort des Clients, um sich an der entsprechenden Datenbank anzumelden.
MetadataAccessConnectString	JDBC-Verbindungs-URL für den Zugriff auf Metadaten in der Datenbank jdbc:informatica:oracle://<host_name>:<port>;SID=<database name>
AdvancedJDBCSecurityOptions	<p>Optional. Datenbankparameter für Metadata-Zugriff auf eine sichere Datenbank. Informatica behandelt den Wert des Felds „AdvancedJDBCSecurityOptions“ als vertrauliche Daten und verschlüsselt die Parameter-Zeichenfolge.</p> <p>Um eine Verbindung zu einer sicheren Datenbank herzustellen, beziehen Sie die folgenden Parameter mit ein:</p> <ul style="list-style-type: none"> <li>- EncryptionMethod. Erforderlich. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf SSL festgelegt werden.</li> <li>- ValidateServerCertificate. Optional. Gibt an, ob Informatica das Zertifikat validiert, das vom Datenbankserver gesendet wird. Wenn dieser Parameter auf „true“ gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den HostNameInCertificate-Parameter angeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat. Wenn dieser Parameter auf "false" festgelegt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben.</li> <li>- HostNameInCertificate. Optional. Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, validiert Informatica den Hostnamen in der Verbindungszeichenfolge mit dem Hostnamen im SSL-Zertifikat.</li> <li>- TrustStore. Erforderlich. Pfad und Dateiname der Truststore-Datei, die das SSL-Zertifikat für die Datenbank enthält.</li> <li>- TrustStorePassword Erforderlich. Passwort der Truststore-Datei für die sichere Datenbank.</li> <li>- KeyStore. Erforderlich. Pfad und Dateiname der Schlüsselspeicherdatei.</li> <li>- KeyStorePassword. Passwort der Schlüsselspeicherdatei für die sichere Datenbank.</li> </ul> <p><b>Hinweis:</b> Eine vollständige Liste der sicheren JDBC-Parameter finden Sie in der DataDirect JDBC-Dokumentation.</p> <p>Informatica hängt die sichere JDBC-Parameter an die Verbindungszeichenfolge an. Wenn Sie die sicheren JDBC-Parameter direkt in der Verbindungszeichenfolge einschließen, geben Sie keinen Parameter in das Feld AdvancedJDBCSecurityOptions ein.</p>
DataAccessConnectString	Verbindungszeichenfolge für den Zugriff auf Daten in der Datenbank Geben Sie die Verbindungszeichenfolge im folgenden Format aus dem TNSNAMES-Eintrag ein:  <Datenbankname>
CodePage	Erforderlich. Codepage, die zum Lesen aus einer Quelldatenbank oder zum Schreiben in eine Zieldatenbank oder -Datei verwendet wird.

Option	Beschreibung
EnvironmentSQL	Optional. SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt. <b>Beispiel:</b> <code>ALTER SESSION SET CURRENT_SCHEMA=INFA_USR;</code> <b>Hinweis:</b> Setzen Sie Sonderzeichen in doppelte Anführungszeichen.
TransactionSQL	Optional. SQL-Befehle zum Ausführen vor jeder Transaktion. Der Datenintegrationsdienst führt die Transaktions-SQL am Anfang jeder Transaktion aus. <b>Beispiel:</b> <code>SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;</code> <b>Hinweis:</b> Setzen Sie Sonderzeichen in doppelte Anführungszeichen.
EnableParallelMode	Optional. Ermöglicht Parallelverarbeitung beim Laden von Daten in eine Tabelle im Massenmodus. Wird für Oracle verwendet. „True“ oder „False“. Standardwert ist „False“.
QuoteChar	Optional. Das Zeichen, das als Anführungszeichen in dieser Verbindung verwendet wird. Der Zeichentyp, der zur Kennzeichnung von Sonderzeichen und reservierten SQL-Schlüsselwörtern, wie WHERE, verwendet wird. Der Datenintegrationsdienst schließt mit dem ausgewählten Zeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Der Datenintegrationsdienst verwendet dieses Zeichen auch für die Eigenschaft „QuoteChar“. Standardwert ist 0.
EnableQuotes	Optional. Wählen Sie diesen Wert, um Anführungszeichen für diese Verbindung zu aktivieren. Sofern aktiviert, schließt der Datenintegrationsdienst Tabellen-, Ansichts-, Schema-, Synonym- und Spaltennamen in Bezeichnerzeichen ein, wenn SQL für diese Objekte in der Verbindung erzeugt und ausgeführt wird. Zu verwenden, wenn Objekte Namen mit gemischter Groß-/Kleinschreibung oder kleingeschriebene Namen haben. Gültige Werte sind „True“ oder „False“. Standardwert ist „True“.
EnableConnectionPool	Optional. Aktiviert das Verbindungspooling. Wenn Sie Verbindungspooling aktivieren, behält der Verbindungspool inaktive Verbindungsinstanzen im Speicher. Wenn Sie Verbindungspooling deaktivieren, stoppt der Datenintegrationsdienst alle Poolingaktivitäten. Gültige Werte sind „True“ oder „False“. Standardwert ist „True“.
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Datenintegrationsdienst für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Standardwert ist 15.
ConnectionPoolMaxIdleTime	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird. Standardwert ist 120.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Standardwert ist 0.

## Salesforce-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Salesforce-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

... -o option\_name=value option\_name=value ...

Beispiel für eine Salesforce-Verbindung, die `infacmd` verwendet

```
infacmd createConnection -dn DomainName -un Domain_UserName -pd Domain_Pwd -cn
Connection_Name -cid Connection_ID -ct SALESFORCE -o userName=salesforceUserName
password=salesforcePWD SERVICE_URL=https://login.salesforce.com/services/Soap/u/42.0
```

Beispiel für eine OAuth Salesforce-Verbindung, die `pmcmd` verwendet

```
pmcmd createConnection -s Salesforce -n ConnectionName -u -p -l CodePage -k
ConnectionType=OAuth RefreshToken=salesforceRefreshToken
ConsumerKey=salesforceConsumerKey ConsumerSecret= salesforceConsumerSecret
Service_URL=https://login.salesforce.com/services/Soap/u/42.0
```

Beispiel für eine Standard Salesforce-Verbindung, die `pmcmd` verwendet

```
pmcmd createConnection -s Salesforce -n ConnectionName -u salesforceUserName -p
salesforcePWD -l CodePage -k ConnectionType=Standard Service_URL=https://
login.salesforce.com/services/Soap/u/42.0
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Salesforce-Verbindungsoptionen für `infacmd` `isp` `CreateConnection`- und `UpdateConnection`-Befehle beschrieben:

Option	Beschreibung
Benutzername	Salesforce-Benutzername.
Passwort	Passwort für den Salesforce-Benutzernamen. Beim Passwort wird die Groß-/ Kleinschreibung beachtet. Um auf Salesforce von außerhalb des vertrauenswürdigen Netzwerks Ihres Unternehmens zuzugreifen, müssen Sie einen Sicherheitstoken an Ihr Passwort anhängen, um sich bei der API oder einem Desktop-Client anzumelden. Um Ihren Sicherheitstoken zu erhalten oder zurückzusetzen, melden Sie sich bei Salesforce an und klicken auf <b>Setup (Einrichten) &gt; My Personal Information (Meine persönlichen Daten) &gt; Reset My Security Token (Meinen Sicherheitstoken zurücksetzen)</b> .
Aktualisierungs-Token	Für eine OAuth Salesforce-Verbindung. Der Aktualisierungs-Token von Salesforce, der unter Verwendung des Verbraucherschlüssels und -geheimworts erzeugt wird.
Verbraucherschlüssel	Für eine OAuth Salesforce-Verbindung. Der von Salesforce bereitgestellte Verbraucherschlüssel, der zum Erzeugen des Aktualisierungs-Tokens benötigt wird. Weitere Informationen zum Erzeugen des Verbraucherschlüssels finden Sie in der Salesforce-Dokumentation.
Verbrauchergeheimwort	Für eine OAuth Salesforce-Verbindung. Das von Salesforce bereitgestellte Verbrauchergeheimwort, das zum Erzeugen des Aktualisierungs-Tokens benötigt wird. Weitere Informationen zum Erzeugen des Verbrauchergeheimworts finden Sie in der Salesforce-Dokumentation.

Option	Beschreibung
Verbindungstyp	Wählen Sie die Standard oder OAuth Salesforce-Verbindung aus.
Dienst-URL	URL des Salesforce-Diensts, auf den Sie zugreifen möchten. In einer Test- oder Entwicklungsumgebung möchten Sie möglicherweise auf die Salesforce-Sandbox-Testumgebung zugreifen. Weitere Informationen zur Salesforce-Sandbox finden Sie in der Salesforce-Dokumentation.

## Salesforce Marketing Cloud-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Salesforce Marketing Cloud-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Beispiel für den Befehl „infacmd createConnection“:

```
./infacmd.sh createConnection -dn DomainName -un Domain_UserName -pd Domain_Pwd -cn
Connection_Name -cid Connection_ID -ct SFMC -o salesforce_marketing_cloud_url=https://
webservice.s7.exacttarget.com/etframework.wsdl userName=SFMCUserName password=SFMCpwd
clientid=SFMCclientid clientsecret=SFMCclientsecret enable_logging=true UTC_Offset=UTC+05:30
Batch_Size=1
```

Beispiel für den Befehl „infacmd updateConnection“:

```
./infacmd.sh updateConnection -dn DomainName -un Domain_UserName -pd Domain_Pwd -cn
Connection_Name -o salesforce_marketing_cloud_url=https://
mc6tbszr9y72l86wknwg5w3c3k7q.soap.marketingcloudapis.com/etframework.wsdl
userName=SFMCUserName password=SFMCpwd clientid=SFMCclientid clientsecret=SFMCclientsecret
enable_logging=true UTC_Offset=UTC+05:30 Batch_Size=1
```

Beispiel für den Befehl „infacmd removeConnection“:

```
./infacmd.sh removeConnection -dn DomainName -un Domain_UserName -pd Domain_Pwd -cn
Connection_Name
```

In der folgenden Tabelle werden die Salesforce Marketing Cloud-Verbindungsoptionen für die Befehle „infacmd.sh createConnection“ und „infacmd.sh updateConnection“ und für remove-Befehle beschrieben:

Verbindungseigenschaft	Beschreibung
Domänenname	Die Informatica-Domäne, in der Sie die Verbindung erstellen möchten.
Domänen-Benutzername	Benutzername der Domäne.
Domänenpasswort	Passwort für die Domäne.
Verbindungsname	Name der Salesforce Marketing Cloud-Verbindung.
Verbindungs-ID	Der Datenintegrationsdienst verwendet die ID zum Erkennen der Verbindung.



Verbindungseigenschaft	Beschreibung
URL der Salesforce Marketing Cloud	<p>Die URL, die der Datenintegrationsdienst zum Herstellen einer Verbindung zu Salesforce Marketing Cloud-WSDL verwendet.</p> <p>Folgende URL ist ein Beispiel für OAuth 1.0 URL:  <code>https://webservice.s7.exacttarget.com/etframework.wsdl</code></p> <p>Folgende URL ist ein Beispiel für OAuth 2.0 URL:  <code>https://&lt;SUBDOMÄNE&gt;.soap.marketingcloudapis.com/etframework.wsdl</code></p> <p>Informatica empfiehlt, dass Sie ein Upgrade auf OAuth 2.0 durchführen, bevor Salesforce Marketing Cloud die Unterstützung für OAuth 1.0 einstellt.</p>
Benutzername	Benutzername des Salesforce Marketing Cloud-Kontos.
Passwort	Passwort für das Salesforce Marketing Cloud-Konto.
Client-ID	Für die Client-ID von Salesforce Marketing Cloud ist das Generieren eines gültigen Zugriffstokens erforderlich.
Geheimer Clientschlüssel	Für den geheimen Schlüssel des Clients von Salesforce Marketing Cloud ist das Generieren eines gültigen Zugriffstokens erforderlich.
Protokollierung aktivieren	Wenn Sie die Protokollierung aktivieren, können Sie das Sitzungsprotokoll für die Aufgaben sehen.
UTC-Offset	Der Sicherheitsagent verwendet die UTC-Offset-Verbindungseigenschaft, um Daten in der UTC-Offset-Zeitzone von der Salesforce Marketing Cloud zu lesen und in sie zu schreiben.
Batch-Größe	<p>Anzahl der Zeilen, die der Sicherheitsagent in einem Batch in das Ziel schreibt.</p> <p>Wenn Sie Daten einfügen oder aktualisieren und den Kontaktschlüssel angeben, werden die der angegebenen Kontakt-ID zugeordneten Daten in einem Batch in der Salesforce Marketing Cloud eingefügt oder aktualisiert. Geben Sie bei einem Upsert der Daten nach Salesforce Marketing Cloud keinen Kontaktschlüssel an.</p>

## SAPAPPLICATIONS-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren der SAPAPPLICATIONS-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die SAPAPPLICATIONS-Verbindungsoptionen für die Befehle „infacmd isp CreateConnection“ und „infacmd isp UpdateConnection“ beschrieben:

Option	Beschreibung
UserName	Erforderlich. SAP-Systembenutzername.
Passwort	Erforderlich. Passwort für den Benutzernamen.
HostName	Erforderlich. Hostname der SAP-Anwendung.
ClientNumber	Erforderlich. SAP-Clientnummer.
SystemNumber	Erforderlich. SAP-Systemnummer.
Sprache	Optional. SAP-Anmeldesprache.

## Sequentielle Verbindungs-Optionen

Verwenden Sie SEQ-Verbindungsoptionen zum Definieren einer Verbindung zu einem sequentiellen z/OS-Datensatz.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die SEQ-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
CodePage	Erforderlich. Code zum Lesen aus der sequentiellen Datei oder zum Schreiben in diese Datei. Verwenden Sie den ISO-Codepage-Namen, z. B. ISO-8859-6. Der Codepage-Name berücksichtigt keine Groß- und Kleinschreibung.
ArraySize	Optional. Bestimmt die Anzahl der Datensätze im Speicher-Array für die Threads, wenn der Worker-Threads-Wert größer als 0 ist. Gültige Werte sind 1 bis 5000. Standardwert ist 25.
Komprimierung	Optional. Komprimiert die Daten, um die Menge an Daten zu reduzieren, die Informatica-Anwendungen über das Netzwerk schreiben. „True“ oder „False“. Standardwert ist „False“.
EncryptionLevel	Optional. Verschlüsselungsebene. Wenn Sie AES für die Option EncryptionType angeben, müssen Sie einen der folgenden Werte angeben, um die Ebene der AES-Verschlüsselung anzugeben: <ul style="list-style-type: none"> <li>- 1. Verwenden Sie einen 128-Bit-Verschlüsselungsschlüssel.</li> <li>- 2. Verwenden Sie einen 192-Bit-Verschlüsselungsschlüssel.</li> <li>- 3. Verwenden Sie einen 256-Bit-Verschlüsselungsschlüssel.</li> </ul> Standardwert ist 1. <b>Hinweis:</b> Wenn Sie für den Verschlüsselungstyp „Keine“ auswählen, ignoriert der Datenintegrationsdienst den Wert für die Verschlüsselungsebene.

Option	Beschreibung
EncryptionType	<p>Optional. Geben Sie einen der folgenden Werte für den Verschlüsselungstyp ein:</p> <ul style="list-style-type: none"> <li>- Keine</li> <li>- AES</li> </ul> <p>Standardwert ist „Keine“.</p> <p>Optional. Steuert, ob Verschlüsselung verwendet werden soll. Geben Sie einen der folgenden Werte an:</p> <ul style="list-style-type: none"> <li>- Keine</li> <li>- AES</li> </ul> <p>Standardwert ist „Keine“.</p>
InterpretAsRows	Optional. Bei TRUE gibt die Pacing-Größe eine Anzahl von Zeilen wieder. Bei „false“ gibt die Pacing-Größe Kilobyte wieder. Standardwert ist „false“.
Speicherort:	Speicherort des PowerExchange Listener-Knotens, der eine Verbindung zur Datenquelle herstellen kann. Der Speicherort ist im ersten Parameter der NODE-Anweisung in der PowerExchange-Konfigurationsdatei „dbmover.cfg“ angegeben.
OffLoadProcessing	<p>Optional. Verschiebt die Stapeldatenverarbeitung vom Datenquellcomputer zu dem Computer, auf dem der Datenintegrationsdienst ausgeführt wird.</p> <p>Geben Sie einen der folgenden Werte ein:</p> <ul style="list-style-type: none"> <li>- Auto. Der Datenintegrationsdienst bestimmt, ob Offload-Verarbeitung verwendet werden soll.</li> <li>- Ja. Offload-Verarbeitung wird verwendet.</li> <li>- Nein. Offload-Verarbeitung wird nicht verwendet.</li> </ul> <p>Standardwert ist „Auto“.</p>
PacingSize	Optional. Verlangsamt die Datenübertragungsrate, um Engpässe zu reduzieren. Je geringer der Wert ist, desto höher ist die Sitzungsleistung. Der Mindestwert lautet 0. Geben Sie 0 für optimale Leistung ein. Standardwert ist 0.
WorkerThread	Optional. Anzahl der vom Datenintegrationsdienst verwendeten Threads, um Stapeldaten bei aktivierter Offload-Verarbeitung zu verarbeiten. Um eine optimale Leistung zu erzielen, sollte dieser Wert die Anzahl der verfügbaren Prozessoren auf dem Rechner des Datenintegrationsdienstes nicht überschreiten. Gültige Werte sind 1 bis 64. Standardwert ist 0, wodurch Multithreading deaktiviert wird.
WriteMode	<p>Geben Sie einen der folgenden Schreibmodi ein:</p> <ul style="list-style-type: none"> <li>- CONFIRMWRITEON. Sendet Daten zum Data Integration Service und wartet auf eine Erfolgs-/Nichterfolgsreaktion, bevor weitere Daten gesendet werden.</li> <li>- CONFIRMWRITEOFF. Sendet Daten zum Data Integration Service, ohne eine Erfolgs-/Nichterfolgsreaktion abzuwarten. Verwenden Sie diese Option, wenn die Target-Tabelle bei Auftreten eines Fehlers erneut geladen werden kann.</li> <li>- ASYNCHRONOUSWITHFAULTT. Sendet Daten asynchron zum Data Integration Service mit der Möglichkeit der Fehlererkennung.</li> </ul> <p>Der Standardwert ist CONFIRMWRITEON.</p>
EnableConnectionPool	Optional. Aktiviert das Verbindungspooling. Wenn Sie Verbindungspooling aktivieren, behält der Verbindungspool inaktive Verbindungsinstanzen im Speicher. Wenn Sie Verbindungspooling deaktivieren, stoppt der Datenintegrationsdienst alle Poolingaktivitäten. „True“ oder „False“. Standardwert ist „False“.
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Datenintegrationsdienst für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Standardwert ist 15.

Option	Beschreibung
ConnectionPoolMaxIdle Time	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird. Standardwert ist 120.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Standardwert ist 0.

## Snowflake-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Snowflake-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

... -o option\_name=value option\_name=value ...

Beispiel:

```
./infacmd.sh createconnection -dn Domain Snowflake -un Administartor -pd Administrator -cn Snowflake_CLI -ct SNOWFLAKE -o "user=INFAADPQA password=passwd account=informatica role=ROLE_PC_AUTO warehouse=QAAUTO_WH"
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Um einen Wert einzugeben, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Wert in Anführungszeichen.

In der folgenden Tabelle werden die obligatorischen Snowflake-Verbindungsoptionen für die Befehle „infacmd isp CreateConnection“ und „UpdateConnection“ beschrieben:

Eigenschaft	Beschreibung
connectionId	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet.
connectionType	Der Verbindungstyp. Verbindungstyp lautet Snowflake.
name	Der Name der Verbindung.
account	Der Name des Snowflake-Kontos.
additionalparam	Geben Sie einen oder mehrere JDBC-Verbindungsparameter in folgendem Format ein: <param1>=<value>&<param2>=<value>&<param3>=<value>... Beispiel: user=jon&warehouse=mywh&db=mydb&schema=public
password	Das Passwort zum Herstellen einer Verbindung zum Snowflake-Konto.
role	Die dem Benutzer zugewiesene Snowflake-Rolle.
user	Der Benutzername zum Herstellen einer Verbindung mit dem Snowflake-Konto.
warehouse	Der Name des Snowflake-Warehouses.

## Tableau-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Tableau-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Beispiel:

```
./infacmd.sh createconnection -dn Domain -un Username -pd Password -cn Connection name -  
ct TABLEAU -o "connectionURL= contentURL= password= tableauProduct='Tableau Server'  
username=infaadmin site='' tabcmdInstallLocation='' tableauServer=true"
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Um einen Wert einzugeben, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Wert in Anführungszeichen.

In der folgenden Tabelle werden die obligatorischen Tableau-Verbindungsoptionen für die Befehle „infacmd isp CreateConnection“ und „UpdateConnection“ beschrieben:

Verbindungseigenschaft	Beschreibung
Tableau-Produkt	Der Name des Tableau-Produkts, zu dem Sie eine Verbindung herstellen möchten. Zum Veröffentlichen der TDE- oder TWBX-Datei können Sie eines der folgenden Tableau-Produkte auswählen: <ul style="list-style-type: none"><li>- Tableau Desktop. Erstellt eine TDE-Datei auf dem Computer des Datenintegrationsdiensts. Sie können dann die TDE-Datei manuell in Tableau Desktop importieren.</li><li>- Tableau Server. Veröffentlicht die generierte TDE- oder TWBX-Datei auf Tableau Server.</li><li>- Tableau Online. Veröffentlicht die generierte TDE- oder TWBX-Datei auf Tableau Online.</li></ul>
URL der Verbindung	URL von Tableau Server oder Tableau Online, unter der Sie die TDE- oder TWBX-Datei veröffentlichen möchten. Die URL hat folgendes Format: <code>http://&lt;Hostname von Tableau Server oder Tableau Online&gt;:&lt;port&gt;</code>
Benutzername	Benutzername des Tableau Server- oder Tableau Online-Kontos.
Passwort	Passwort für das Tableau Server- oder Tableau Online-Konto.
Inhalts-URL	Der Name der Website auf Tableau Server oder Tableau Online, auf der Sie die TDE- oder TWBX-Datei veröffentlichen möchten. Wenden Sie sich an den Tableau-Administrator, um den Namen der Website bereitzustellen.

## Tableau V3-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Tableau V3-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Beispiel:

```
./infacmd.sh createConnection -dn Domain -un Username -pd Password -cn Connection name -  
ct tableau_server -ct TABLEAU V3 -o "connectionURL= site= password=  
tableauProduct='Tableau Server' username="
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die obligatorischen Tableau V3-Verbindungsoptionen für die Befehle „infacmd isp CreateConnection“ und „UpdateConnection“ beschrieben:

Verbindungseigenschaft	Beschreibung
Tableau-Produkt	<p>Der Name des Tableau-Produkts, zu dem Sie eine Verbindung herstellen möchten. Zum Veröffentlichen der .hyper- oder TWBX-Datei können Sie eines der folgenden Tableau-Produkte auswählen:</p> <p><b>Tableau Desktop</b></p> <p>Erstellt eine .hyper-Datei auf dem Computer des Datenintegrationsdiensts. Sie können die .hyper-Datei dann manuell in Tableau Desktop importieren.</p> <p><b>Tableau Server</b></p> <p>Veröffentlicht die generierte .hyper- oder TWBX-Datei auf Tableau Server.</p> <p><b>Tableau Online</b></p> <p>Veröffentlicht die generierte .hyper- oder TWBX-Datei auf Tableau Online.</p>
URL der Verbindung	<p>URL von Tableau Server oder Tableau Online, unter der Sie die .hyper- oder TWBX-Datei veröffentlichen möchten.</p> <p>Geben Sie die URL in folgendem Format ein: <code>http://&lt;Hostname von Tableau Server oder Tableau Online&gt;:&lt;port&gt;</code></p>
Benutzername	Der Benutzername des Kontos für Tableau Server bzw. Tableau Online.
Passwort	Das Passwort für das Tableau Server- oder Tableau Online-Konto.
Site-ID	<p>Die ID der Website auf Tableau Server oder Tableau Online, auf der Sie die TWBX-Datei veröffentlichen möchten.</p> <p><b>Hinweis:</b> Bitten Sie den Tableau-Administrator, die ID der Website bereitzustellen.</p>
Dateipfad für Schema	<p>Der Pfad der .hyper-Beispieldatei, aus der der Datenintegrationsdienst die Tableau-Metadaten importiert.</p> <p>Geben Sie eine der folgenden Optionen für den Pfad der Schemadatei ein:</p> <ul style="list-style-type: none"> <li>- Absoluter Pfad der .hyper-Datei.</li> <li>- Verzeichnispfad der .hyper-Dateien.</li> <li>- Leerer Verzeichnispfad.</li> </ul> <p>Der für die Schemadatei angegebene Pfad wird zum Standardpfad der .hyper-Zieldatei. Wenn Sie keinen Dateipfad angeben, verwendet der Datenintegrationsdienst den folgenden Standarddateipfad für die .hyper-Zieldatei:</p> <p><code>&lt;Installationsverzeichnis des Datenintegrationsdiensts&gt;/apps/Data_Integration_Server/&lt;latest version&gt;/bin/rtdm</code></p>

## Verbindungsoptionen des parallelen Teradata-Transporters

Verwenden Sie Verbindungsoptionen zur Definition einer Teradata-PT-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name='value' option_name='value' ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Die folgende Tabelle beschreibt die Optionen der Teradata-PT-Verbindung für infacmd isp CreateConnection- und UpdateConnection-Befehle:

Option	Beschreibung
UserName	Erforderlich. Benutzername der Teradata-Datenbank mit den entsprechenden Schreibberechtigung zum Zugriff auf die Datenbank.
Passwort	Erforderlich. Passwort für den Benutzernamen der Teradata-Datenbank.
DriverName	Erforderlich. Name des Teradata-JDBC-Treibers.
ConnectionString	Erforderlich. JDBC-URL zum Abrufen von Metadaten.
TDPID	Erforderlich. Name oder IP-Adresse des Teradata-Datenbankcomputers.
databaseName	Erforderlich. Teradata-Datenbankname. Wenn Sie keinen Datenbanknamen eingeben, verwendet die Teradata-PT-API den Standardanmeldungsnamen der Datenbank.
DataCodePage	Optional. Codepage, die mit der Datenbank verbunden ist. Beim Ausführen eines Mappings, das ein Teradata-Target lädt, muss die Codepage der Teradata-PT-Verbindung mit der Codepage des Teradata-Target übereinstimmen. Standardwert ist UTF-8.
Beharrlichkeit	Optional. Anzahl der Stunden, in denen die Teradata-PT-API weiterhin versucht, sich anzumelden, wenn die maximale Anzahl von Operationen in der Teradata-Datenbank ausgeführt wird. Muss ein positiver, ganzzahliger Wert sein, der nicht Null ist. Standardwert ist 4.
MaxSessions	Optional. Maximale Anzahl der Sitzungen, die die Teradata-PT-API mit der Teradata-Datenbank herstellt. Muss ein positiver, ganzzahliger Wert sein, der nicht Null ist. Standardwert ist 4.
MinSessions	Optional. Mindestanzahl von Teradata-PT-API-Sitzungen, die erforderlich ist, damit der Teradata-PT-API-Job fortfährt. Muss ein positiver, ganzzahliger Wert zwischen 1 und dem maximalen Wert für Sitzungen sein. Standardwert ist 1.
Ruhezustand	Optional. Anzahl der Minuten, in denen die Teradata-PT-API anhält, bevor sie wieder versucht, sich anzumelden, wenn die maximale Anzahl von Operationen in der Teradata-Datenbank ausgeführt wird. Muss ein positiver, ganzzahliger Wert sein, der nicht Null ist. Standardwert ist 6.
useMetadataJdbcUrl	Optional. Legen Sie diese Option auf TRUE fest, um anzugeben, dass der TDCH (Teradata Connector for Hadoop) die JDBC-URL verwenden muss, die in der Verbindungszeichenfolge angegeben wurde. Legen Sie diese Option auf FALSE fest, um eine andere JDBC-URL anzugeben, die vom TDCH bei der Ausführung der Zuordnung verwendet werden muss.

Option	Beschreibung
tdchJdbcUrl	Erforderlich. JDBC-URL, die TDCH beim Ausführen der Zuordnung verwenden muss.
dataEncryption	Erforderlich. Aktiviert vollständige Sicherheitsverschlüsselung von SQL-Abfragen, Antworten und Daten unter Windows. Fügen Sie zur Aktivierung von Verschlüsselung unter UNIX den Befehl <code>UseDataEncryption=Yes</code> zum DNS in der Datei „odbc.ini“ hinzu.
authenticationType	Erforderlich. Authentifiziert den Benutzer. Geben Sie die folgenden Werte für den Authentifizierungstyp ein: <ul style="list-style-type: none"> <li>- Nativ. Authentifiziert den Benutzernamen und das Kennwort für die in der Verbindung angegebene Teradata-Datenbank.</li> <li>- LDAP. Authentifiziert Benutzeranmeldeinformationen für den externen LDAP-Verzeichnisdienst.</li> </ul> Standardwert ist „Nativ“.
hadoopConnector	Erforderlich, wenn Sie Sqoop-Konnektivität für das Datenobjekt aktivieren möchten, das die JDBC-Verbindung verwendet. Der Datenintegrationsdienst führt das Mapping in der Hadoop-Laufzeitumgebung über Sqoop aus. Sie können Sqoop-Konnektivität für relationale Datenobjekte, benutzerdefinierte Datenobjekte und logische Datenobjekte konfigurieren, die auf einer JDBC-fähigen Datenbank basieren. Legen Sie den Wert auf <code>SQOOP_146</code> fest, um Sqoop-Konnektivität zu aktivieren.
hadoopConnectorArgs	Optional. Geben Sie die Argumente ein, die von Sqoop zum Herstellen einer Verbindung zur Datenbank verwendet werden müssen. Schließen Sie die Sqoop-Argumente in einfache Anführungszeichen ein. Trennen Sie mehrere Argumente durch ein Leerzeichen. Beispiel: <code>hadoopConnectorArgs='--&lt;Sqoop-Argument 1&gt; --&lt;Sqoop-Argument 2&gt;'</code> Zum Lesen von Daten aus bzw. Schreiben von Daten in Teradata über spezielle TDCH-Konnektoren (Teradata Connector for Hadoop) für Sqoop definieren Sie die Klasse der TDCH-Verbindungs-Factory im Argument „hadoopConnectorArgs“. Die Klasse der Verbindungs-Factory richtet sich nach dem TDCH-Sqoop-Konnektor, der verwendet werden soll. <ul style="list-style-type: none"> <li>- Zur Verwendung von Cloudera Connector Powered by Teradata konfigurieren Sie das Argument „hadoopConnectorArgs“ folgendermaßen:  <pre>hadoopConnectorArgs='- Dsqaop.connection.factories=com.cloudera.connector.teradata.TeradataManagerFactory'</pre> </li> <li>- Zur Verwendung von Hortonworks Connector for Teradata (unterstützt von Teradata Connector for Hadoop) konfigurieren Sie das Argument „hadoopConnectorArgs argument“ folgendermaßen:  <pre>hadoopConnectorArgs='- Dsqaop.connection.factories=org.apache.sqaop.teradata.TeradataManagerFactory'</pre> </li> </ul> Wenn Sie keine Sqoop-Argumente eingeben, erstellt der Datenintegrationsdienst den Sqoop-Befehl basierend auf den JDBC-Verbindungseigenschaften.



## Twitter-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Twitter-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Twitter-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
ConsumerKey	Der Verbraucherschlüssel, den Sie beim Erstellen der Anwendung in Twitter erhalten. Twitter verwendet die Schlüssel zur Identifizierung der Anwendung.
ConsumerSecret	Das Verbrauchergeheimwort, das Sie beim Erstellen einer Twitter-Anwendung erhalten. Twitter verwendet das Geheimwort für das Eigentum am Verbraucherschlüssel.
AccessToken	Zugriffstoken, den das OAuth-Dienstprogramm zurückgibt. Twitter verwendet diesen Token anstelle der Benutzeranmeldedaten für den Zugriff auf geschützte Ressourcen.
AccessSecret	Zugriffsgeheimwort, das das OAuth-Dienstprogramm zurückgibt. Das Geheimwort legt das Eigentum eines Token fest.

## Twitter Streaming-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Twitter Streaming-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Twitter Streaming-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
HoseType	Streaming-API-Methoden. Sie können die folgenden Methoden angeben: <ul style="list-style-type: none"><li>- Filter. Die Twitter <code>statuses/filter</code>-Methode gibt öffentliche Statusangaben zurück, die mit den Suchkriterien übereinstimmen.</li><li>- Beispiel. Die Twitter <code>statuses/sample</code>-Methode gibt eine zufällige Stichprobe aus allen öffentlichen Statusangaben zurück.</li></ul>
UserName	Name des Twitter-Benutzerbildschirms
Passwort	Twitter-Passwort.

## VSAM-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer VSAM-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die VSAM-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
CodePage	Erforderlich. Code zum Lesen aus der oder Schreiben in die VSAM-Datei. Verwenden Sie den ISO-Codepage-Namen, z. B. ISO-8859-6. Der Codepage-Name berücksichtigt keine Groß- und Kleinschreibung.
ArraySize	Optional. Bestimmt die Anzahl der Datensätze im Speicher-Array für die Threads, wenn der Worker-Threads-Wert größer als 0 ist. Gültige Werte sind 1 bis 5000. Standardwert ist 25.
Komprimierung	Optional. Komprimiert die Daten, um die Menge an Daten zu reduzieren, die Informatica-Anwendungen über das Netzwerk schreiben. „True“ oder „False“. Standardwert ist „False“.
EncryptionLevel	Optional. Verschlüsselungsebene. Wenn Sie AES für die Option EncryptionType angeben, müssen Sie einen der folgenden Werte angeben, um die Ebene der AES-Verschlüsselung anzugeben: <ul style="list-style-type: none"> <li>- 1. Verwenden Sie einen 128-Bit-Verschlüsselungsschlüssel.</li> <li>- 2. Verwenden Sie einen 192-Bit-Verschlüsselungsschlüssel.</li> <li>- 3. Verwenden Sie einen 256-Bit-Verschlüsselungsschlüssel.</li> </ul> Standardwert ist 1. <b>Hinweis:</b> Wenn Sie für den Verschlüsselungstyp „Keine“ auswählen, ignoriert der Datenintegrationsdienst den Wert für die Verschlüsselungsebene.
EncryptionType	Optional. Steuert, ob Verschlüsselung verwendet werden soll. Geben Sie einen der folgenden Werte an: <ul style="list-style-type: none"> <li>- Keine</li> <li>- AES</li> </ul> Standardwert ist „Keine“.
InterpretAsRows	Optional. Bei TRUE gibt die Pacing-Größe eine Anzahl von Zeilen wieder. Bei „false“ gibt die Pacing-Größe Kilobyte wieder. Standardwert ist „false“.
Speicherort:	Speicherort des PowerExchange Listener-Knotens, der eine Verbindung zu VSAM herstellen kann. Der Knoten wird in der dbmover.cfg-Konfigurationsdatei von PowerExchange definiert.
OffLoadProcessing	Optional. Verschiebt die Stapeldatenverarbeitung von der VSAM-Quelle zum Datenintegrationsdienst-Computer. Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- Auto. Der Datenintegrationsdienst bestimmt, ob Offload-Verarbeitung verwendet werden soll.</li> <li>- Ja. Offload-Verarbeitung wird verwendet.</li> <li>- Nein. Offload-Verarbeitung wird nicht verwendet.</li> </ul> Standardwert ist „Auto“.

Option	Beschreibung
PacingSize	Optional. Verlangsamt die Datenübertragungsrate, um Engpässe zu reduzieren. Je geringer der Wert ist, desto höher ist die Sitzungsleistung. Der Mindestwert lautet 0. Geben Sie 0 für optimale Leistung ein. Standardwert ist 0.
WorkerThread	Optional. Anzahl der vom Datenintegrationsdienst verwendeten Threads, um Stapeldaten bei aktivierter Offload-Verarbeitung zu verarbeiten. Um eine optimale Leistung zu erzielen, sollte dieser Wert die Anzahl der verfügbaren Prozessoren auf dem Rechner des Datenintegrationsdienstes nicht überschreiten. Gültige Werte sind 1 bis 64. Standardwert ist 0, wodurch Multithreading deaktiviert wird.
WriteMode	Geben Sie einen der folgenden Schreibmodi ein: <ul style="list-style-type: none"> <li>- CONFIRMWRITEON. Sendet Daten zum Data Integration Service und wartet auf eine Erfolgs-/Nichterfolgsreaktion, bevor weitere Daten gesendet werden.</li> <li>- CONFIRMWRITEOFF. Sendet Daten zum Data Integration Service, ohne eine Erfolgs-/Nichterfolgsreaktion abzuwarten. Verwenden Sie diese Option, wenn die Target-Tabelle bei Auftreten eines Fehlers erneut geladen werden kann.</li> <li>- ASYNCHRONOUSWITHFAULTT. Sendet Daten asynchron zum Data Integration Service mit der Möglichkeit der Fehlererkennung.</li> </ul> Der Standardwert ist CONFIRMWRITEON.
EnableConnectionPool	Optional. Aktiviert das Verbindungspooling. Wenn Sie Verbindungspooling aktivieren, behält der Verbindungspool inaktive Verbindungsinstanzen im Speicher. Wenn Sie Verbindungspooling deaktivieren, stoppt der Datenintegrationsdienst alle Poolingaktivitäten. „True“ oder „False“. Standardwert ist „False“.
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Datenintegrationsdienst für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Standardwert ist 15.
ConnectionPoolMaxIdle Time	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird. Standardwert ist 120.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Standardwert ist 0.

## Verbindungsoptionen von Web Content-Kapow Katalyst

Verwenden Sie die Verbindungsoptionen, um eine Web Content-Kapow Katalyst-Verbindung zu definieren.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Die folgende Tabelle beschreibt die Verbindungsoptionen von Web Content-Kapow Katalyst für infacmd isp CreateConnection- und UpdateConnection-Befehle:

Option	Beschreibung
ManagementConsoleURL	URL der lokalen Management-Konsole, wo der Robot hochgeladen wird. Die URL muss mit http oder https beginnen. Zum Beispiel http://localhost:50080.
RQLServicePort	Die Portnummer, auf der der Socket-Dienst den RQL-Dienst abhört. Geben Sie einen Wert zwischen 1 und 65535 ein. Der Standardwert ist 50000.
Benutzername	Benutzername ist erforderlich, um auf die lokale Management-Konsole zuzugreifen.
Passwort	Passwort für den Zugriff auf die lokale Management-Konsole.

## CreateFolder

Erstellt einen Ordner in der Domäne. Wenn Sie einen Ordner erstellen, erstellt infacmd den Ordner in der Domäne oder einen von Ihnen angegebenen Ordner.

Sie können mit Ordnern Objekte organisieren und die Sicherheit verwalten. Ordner können Knoten, Dienste, Gitter, Lizenzen und andere Ordner enthalten.

Der Befehl „infacmd isp CreateFolder“ verwendet die folgende Syntax:

```
CreateFolder
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-FolderName|-fn> folder_name
<-FolderPath|-fp> full_folder_path
[<-FolderDescription|-fd> description_of_folder]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateFolder“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-FolderName -fn	folder_name	Erforderlich. Name des Ordners. Ordernamen müssen innerhalb eines Ordners bzw. der Domäne eindeutig sein. Sie dürfen maximal 79 Zeichen und keine Leerzeichen enthalten.
-FolderPath -fp	full_folder_path	Erforderlich. Vollständiger Pfad (ohne Domänenname) für die Erstellung des Ordners. Folgendes Format ist erforderlich: <i>/parent_folder/child_folder</i>
-FolderDescription -fd	description_of_folder	Optional. Beschreibung des Ordners. Wenn die Ordnerbeschreibung Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen.

## CreateGrid

Erstellt ein Gitter in der Domäne weist dem Gitter Knoten zu. Erstellen Sie ein Gitter, um Jobs an Dienstprozesse zu verteilen, die auf Knoten im Gitter ausgeführt werden.

Der Befehl „infacmd isp CreateGrid“ verwendet die folgende Syntax:

```
CreateGrid
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GridName|-gn> grid_name
<-NodeList|-nl> node1 node2 ...
[<-FolderPath|-fp> full_folder_path]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateGrid“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GridName -gn	grid_name	Erforderlich. Name des Gitters.

Option	Argument	Beschreibung
-NodeList -nl	node1 node2 ...	Erforderlich. Name des Knotens, den Sie dem Gitter zuweisen möchten.
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, in dem Sie das Gitter erstellen möchten. Folgendes Format ist erforderlich:  <i>/parent_folder/child_folder</i>  Standardwert ist „/“ (die Domäne).

## CreateGroup

Erstellt eine Gruppe in der nativen Sicherheitsdomäne. Sie können Rollen und Berechtigungen zu einer Gruppe in der nativen oder in einer LDAP-Sicherheitsdomäne zuweisen. Die einer Gruppe zugewiesenen Rollen und Berechtigungen legen die Aufgaben fest, die die Benutzer in der Gruppe innerhalb der Domäne durchführen können.

Der Befehl „infacmd isp CreateGroup“ verwendet die folgende Syntax:

```
CreateGroup
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GroupName|-gn> group_name
[<-GroupDescription|-ds> group_description]
```



In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateGroup“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-GroupName -gn	group_name	<p>Erforderlich. Name der Gruppe. Der Gruppenname unterliegt nicht der Groß-/Kleinschreibung und kann 1 bis 80 Zeichen umfassen. Er darf weder Tabulatoren, Zeilenendzeichen noch folgende Sonderzeichen enthalten:</p> <p>, + " \ &lt; &gt; ; / * % ?</p> <p>Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Alle anderen Leerzeichen sind nicht zulässig.</p>
-GroupDescription -ds	group_description	<p>Optional. Beschreibung der Gruppe. Um eine Beschreibung einzugeben, die Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen.</p> <p>Die Beschreibung darf die folgenden Sonderzeichen nicht enthalten:</p> <p>&lt; &gt; "</p>

## CreateIntegrationService

Erstellt einen PowerCenter-Integrationsdienst in einer Domäne.

Der PowerCenter-Integrationsdienst wird standardmäßig aktiviert, wenn Sie ihn erstellen.

Der Befehl „infacmd isp CreateIntegrationService“ verwendet die folgende Syntax:

```
CreateIntegrationService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
[<-FolderPath|-fp> full_folder_path]
<<-NodeName|-nn> node_name|<-GridName|-gn> grid_name>
[<-BackupNodes|-bn> node1 node2 ...]
<-RepositoryService|-rs> repository_service_name
[<-RepositoryUser|-ru> repository_user]
[<-RepositoryPassword|-rp> repository_password]
[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]
[<-ServiceDisable|-sd>]
[<-ServiceOptions|-so> option_name=value ...]
```

```
[<-ServiceProcessOptions|-po> option_name=value ...]
```

```
[<-EnvironmentVariables|-ev> name=value ...]
```

```
[<-LicenseName|-ln> license_name]
```

**Hinweis:** Für infacmd isp CreateIntegrationService dürfen die Optionen -ru, -rp und -rsdn in der Kerberos-Authentifizierung nicht verwendet werden. Wenn Sie diese Optionen im Kerberos-Modus verwenden, schlägt der Befehl fehl.

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateIntegrationService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des PowerCenter-Integrationsdiensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten:  / * ? < > "
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, in dem Sie den Integrationsdienst erstellen möchten. Folgendes Format ist erforderlich:  <i>/parent_folder/child_folder</i> Standardwert ist „/“ (die Domäne).
-NodeName -nn	node_name	Erforderlich, wenn Sie den Gitternamen nicht angeben. Name des Knotens, auf dem der PowerCenter-Integrationsdienst-Prozess ausgeführt werden soll. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, gibt diese Option den Namen des primären Knotens an.  Starten Sie den Integrationsdienst neu, damit die Änderungen wirksam werden.
-GridName -gn	grid_name	Erforderlich, wenn Sie den Knotennamen nicht angeben. Name des Gitters, in dem der PowerCenter-Integrationsdienst-Prozess ausgeführt werden soll.  Starten Sie den PowerCenter-Integrationsdienst neu, um die Änderungen zu übernehmen.
-BackupNodes -bn	node1 node2 ...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Sicherungsknoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.

Option	Argument	Beschreibung
-RepositoryService -rs	repository_service_name	Erforderlich. Name des PowerCenter-Repository-Diensts, von dem der PowerCenter-Integrationsdienst abhängt. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen. Starten Sie den PowerCenter-Integrationsdienst neu, um die Änderungen zu übernehmen.
-RepositoryUser -ru	repository_user	Erforderlich für native und LDAP-Authentifizierung. Benutzername zum Herstellen einer Verbindung zum PowerCenter-Repository. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen. Starten Sie den PowerCenter-Integrationsdienst neu, um die Änderungen zu übernehmen.
-RepositoryPassword -rp	repository_password	Erforderlich für native und LDAP-Authentifizierung. Benutzerpasswort. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -rp festgelegte Passwort Vorrang. Starten Sie den PowerCenter-Integrationsdienst neu, um die Änderungen zu übernehmen.
- RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Erforderlich für LDAP. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der PowerCenter-Repository-Benutzer gehört. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung. Wenn Sie diese Option nicht angeben, setzt der Befehl die Sicherheitsdomäne des Repository-Benutzers auf nativ.
-ServiceDisable -sd	-	Optional. Erstellt einen deaktivierten Dienst. Sie müssen den Dienst aktivieren, bevor Sie ihn ausführen können.
-ServiceOptions -so	option_name=value	Optional. Diensteigenschaften, mit denen definiert wird, wie der PowerCenter-Integrationsdienst ausgeführt wird.
-ServiceProcessOptions -po	option_name=value	Optional. Dienstprozesseigenschaften für den PowerCenter-Integrationsdienst. In einer Umgebung mit Gittern oder mehreren Knoten wendet infacmd diese Eigenschaften auf den primären Knoten, das Gitter und den Backup-Knoten an.

Option	Argument	Beschreibung
-EnvironmentVariables -ev	name=value	Optional. Geben Sie Umgebungsvariablen als PowerCenter-Integrationsdienst-Prozessoptionen an. Möglicherweise möchten Sie zusätzliche Variablen aufnehmen, die für Ihre PowerCenter-Umgebung eindeutig sind.  Starten Sie den Knoten neu, damit die Änderungen wirksam werden.
-LicenseName -ln	license_name	Erforderlich, wenn Sie einen aktivierten Dienst erstellen. Name der Lizenz, die Sie dem PowerCenter-Integrationsdienst zuweisen möchten.  Starten Sie den PowerCenter-Integrationsdienst neu, um die Änderungen zu übernehmen.

## Integrationsdienst-Optionen

Geben Sie Integrationsdienst-Optionen im folgenden Format ein:

```
infacmd CreateIntegrationService ... -so option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Integrationsdienst-Optionen beschrieben:

Option	Beschreibung
\$PMFailureEmailUser	Optional. E-Mail-Adresse des Benutzers, um E-Mail bei fehlerhaftem Abschluss einer Sitzung zu erhalten. Um mehrere Adressen unter Windows einzugeben, verwenden Sie eine Verteilungsliste. Um mehrere Adressen unter UNIX einzugeben, trennen Sie sie durch ein Komma.
\$PMSessionErrorThreshold	Optional. Anzahl der nicht schwerwiegenden Fehler, die der Integrationsdienst vor dem Abbruch der Sitzung zulässt. Der Standardwert lautet „0“ (nicht schwerwiegende Fehler führen nicht zum Anhalten der Sitzung).
\$PMSessionLogCount	Optional. Anzahl der Sitzungsprotokolle, die der Integrationsdienst für die Sitzung archiviert. Der Mindestwert lautet „0“. 0 ist voreingestellt.
\$PMSuccessEmailUser	Optional. E-Mail-Adresse des Benutzers, um E-Mail bei erfolgreichem Abschluss der Sitzung zu empfangen. Um mehrere Adressen unter Windows einzugeben, verwenden Sie eine Verteilungsliste. Um mehrere Adressen unter UNIX einzugeben, trennen Sie sie durch ein Komma.
\$PMWorkflowLogCount	Optional. Anzahl der Arbeitsablaufprotokolle, die der Integrationsdienst für den Arbeitsablauf archiviert. Der Mindestwert lautet „0“. 0 ist voreingestellt.
AggregateTreatNullAsZero	Optional. Behandelt Nullen als NULL in den Aggregatormwandlungen. Der Standardwert lautet „Nein“.

Option	Beschreibung
AggregateTreatRowAsInsert	Optional. Führt Aggregat-Berechnungen vor dem Markieren von Datensätzen zum Einfügen, Aktualisieren, Löschen oder Ablehnen in Update-Strategie-Ausdrücken durch. Der Standardwert lautet „Nein“.
ClientStore	Optional. Geben Sie den Wert für ClientStore mit folgender Syntax ein:  <path>/<filename>  Beispiel:  ./Certs/client.keystore
CreateIndicatorFiles	Optional. Erstellt Indikatordateien beim Ausführen eines Arbeitsablaufs mit einem Einfachdateiziel. Der Standardwert lautet „Nein“.
DataMovementMode	Optional. Modus, mit dem festgelegt wird, wie der Integrationsdienst Zeichendaten verarbeitet: - ASCII - Unicode Der Standardwert ist „ASCII“.
DateFormat	Optional. Datumsformat, das der Integrationsdienst in Protokolleinträgen verwendet. Der Standardwert lautet „DY MON DD HH 24:MI:SS YYYY“.
DateHandling40Compatibility	Optional. Verarbeitet Daten wie in PowerCenter 1.0/PowerMart 4.0. Der Standardwert lautet „Nein“.
DeadlockSleep	Optional. Anzahl der Sekunden, bevor der Integrationsdienst nach einem Datenbank-Deadlock erneut versucht, in die Zieldatenbank zu schreiben. Der Mindestwert lautet „0“. Der Maximalwert lautet 2592000. Der Standardwert lautet „0“ (sofort versuchen, in das Ziel zu schreiben).
ErrorSeverityLevel	Optional. Niedrigste Stufe der Fehlerprotokollierung für Integrationsdienstprotokolle: - Schwerwiegend - Fehler - Warnung - Info - Trace - Debug Der Standardwert lautet „Info“.
ExportSessionLogLibName	Optional. Name der externen Bibliotheksdatei zum Schreiben der Sitzungsprotokollmeldungen.

Option	Beschreibung
FlushGMDWrite	<p>Erforderlich, wenn Sie Sitzungswiederherstellung aktivieren. Bewirkt das Flushen der Sitzungswiederherstellungsdaten für die Wiederherstellungsdatei aus dem Betriebssystempuffer auf Diskette. Geben Sie einen der folgenden Levels an:</p> <ul style="list-style-type: none"> <li>- Auto. Flusht Wiederherstellungsdaten für alle Echtzeitsitzungen mit einer JMS- oder WebSphere MQ-Quelle und einem nicht relationalen Target.</li> <li>- Yes. Flusht Wiederherstellungsdaten für alle Sitzungen.</li> <li>- No. Flusht keine Wiederherstellungsdaten. Wählen Sie diese Option aus, wenn Sie über hochverfügbare externe Systeme verfügen oder wenn Sie die Leistung optimieren müssen.</li> </ul> <p>Der Standardwert ist Auto.</p>
HttpProxyDomäne	Optional. Domäne für die Authentifizierung
HttpProxyPasswort	Erforderlich, wenn der Proxyserver Authentifizierung erfordert. Passwort für den authentifizierten Benutzer
HttpProxyPort	Optional. Portnummer des HTTP-Proxy-Servers
HttpProxyServer	Optional. Name des HTTP-Proxy-Servers
HttpProxyBenutzer	Erforderlich, wenn der Proxyserver Authentifizierung erfordert. Authentifizierter Benutzername für den HTTP-Proxy-Server
IgnoreResourceRequirements	Optional. Ignoriert Ressourcenanforderungen für Aufgaben bei der Verteilung von Aufgaben an die Knoten in einem Gitter. Der Standardwert lautet „Ja“.
JCEProvider	<p>Optional. JCEProvider-Klassennamen zum Unterstützen der NTLM-Authentifizierung.</p> <p>Beispiel:</p> <pre>com.unix.crypto.provider.UnixJCE.</pre>
JoinerSourceOrder6xCompatibility	Optional. Verarbeitet Master- und Detail-Pipelines nacheinander wie in PowerCenter-Versionen vor Version 7.0. Der Standardwert lautet „Nein“.
LoadManagerAllowDebugging	Optional. Erlaubt Ihnen, den Integrationsdienst zum Ausführen von Debugger-Sitzungen über den Designer zu verwenden. Standardwert ist „Ja“.
LogsInUTF8	Optional. Schreibt alle Protokolle mit dem UTF-8-Zeichensatz. Der Standardwert lautet „Ja“ (Unicode) oder „Nein“ (ASCII).
MSExchangeProfile	Optional. Vom Dienststartkonto zum Senden einer E-Mail nach der Sitzung verwendetes Microsoft Exchange-Profil.
MaxLookupSPDBConnections	Optional. Maximale Anzahl an Verbindungen für eine Lookup-Datenbank oder eine Datenbank für gespeicherte Prozeduren beim Starten einer Sitzung. Der Mindestwert lautet „0“. 0 ist voreingestellt.



Option	Beschreibung
MaxMSSQLConnections	Optional. Maximale Anzahl an Verbindungen zu einer Microsoft SQL Server-Datenbank beim Starten einer Sitzung. Der Mindestwert lautet „100“. Der maximale Wert lautet „2.147.483.647“. Standardwert ist 100.
MaxResilienceTimeout	Optional. Maximaler Zeitraum in Sekunden, in dem der Dienst die Ressourcen zwecks Belastbarkeit beibehält. Der Mindestwert lautet 0. Der Maximalwert lautet 2592000. Der Standardwert lautet „180“.
MaxSybaseConnections	Optional. Maximale Anzahl an Verbindungen zu einer Sybase-Datenbank beim Starten einer Sitzung. Der Mindestwert lautet „100“. Der maximale Wert lautet „2.147.483.647“. Standardwert ist 100.
NumOfDeadlockRetries	Optional. Anzahl der Versuche, die der Integrationsdienst nach einem Datenbank-Deadlock unternimmt, erneut in eine Zieldatenbank zu schreiben. Der Mindestwert lautet „10“. Der maximale Wert lautet „1.000.000.000“. Standardwert ist 10.
OperatingMode	Optional. Betriebsmodus für den Integrationsdienst: <ul style="list-style-type: none"> <li>- Normal</li> <li>- Sicher</li> </ul> Der Standardwert lautet „Normal“.
OperatingModeOnFailover	Optional. Betriebsmodus den Integrationsdienst beim Failover des Dienstprozesses: <ul style="list-style-type: none"> <li>- Normal</li> <li>- Sicher</li> </ul> Der Standardwert lautet „Normal“.
OutputMetaDataForFF	Optional. Schreibt den Spaltenheader in die Einfachdateizeile. Der Standardwert lautet „Nein“.
PersistRuntimeStatsToRepo	Optional. Ebene der im Repository gespeicherten Laufzeitinformationen. Geben Sie einen der folgenden Levels an: <ul style="list-style-type: none"> <li>- Keine. Integration Service speichert keine Sitzungs- oder Arbeitsablaufinformationen zur Laufzeit im Repository.</li> <li>- Normal. Integration Service speichert Arbeitsablaufdetails, Aufgabendetails, Sitzungsstatistiken sowie die Quell- und Target-Statistiken im Repository.</li> <li>- Verbose. Integration Service speichert Arbeitsablaufdetails, Aufgabendetails, Sitzungsstatistiken, Quell- und Target-Statistiken, Partitionsdetails und Leistungsdetails im Repository.</li> </ul> Der Standardwert lautet „Normal“.
Pmserver3XCompatibility	Optional. Verarbeitet Aggregatormwandlungen wie der PowerMart-Server in PowerMart 3.5. Der Standardwert lautet „Nein“.
RunImpactedSessions	Optional. Führt Sitzungen aus, die von den Abhängigkeits-Aktualisierungen beeinflusst sind. Der Standardwert lautet „Nein“.

Option	Beschreibung
ServiceResilienceTimeout	Optional. Zeitraum in Sekunden, in dem der Dienst versucht, eine Verbindung zu einem anderen Dienst herzustellen oder erneut herzustellen. Der Mindestwert lautet 0. Der Maximalwert lautet 2592000. Der Standardwert lautet „180“.
StoreHAPersistenceInDB	Optional. Speichert Informationen zum Prozessstatus in Persistenzdatenbanktabellen der zugehörigen PowerCenter-Repository-Datenbank. Der Standardwert lautet „Nein“.
TimestampWorkflowLogMessages	Optional. Hängt einen Zeitstempel für die in das Arbeitsablaufprotokoll geschriebenen Nachrichten an. Der Standardwert lautet „Nein“.
TreatCharAsCharOnRead	Optional. Behält nachgestellte Leerzeichen beim Lesen von SAP- oder PeopleSoft CHAR-Daten bei. Der Standardwert lautet „Ja“.
TreatDBPartitionAsPassThrough	Optional. Verwendet Pass-Through-Partitionierung für Nicht-DB2-Ziele, wenn es sich um den Partitionstyp „Datenbankpartitionierung“ handelt. Der Standardwert lautet „Nein“.
TreatNullInComparisonOperatorsAs	Optional. Legt fest, wie der Integrationsdienst Nullwerte in Vergleichsoperationen bewertet: <ul style="list-style-type: none"> <li>- Null</li> <li>- Low</li> <li>- High</li> </ul> Der Standardwert lautet „Null“.
TrustStore	Optional. Geben Sie den Wert für TrustStore mit der folgenden Syntax ein: <path>/<filename> Beispiel: ./Certs/trust.keystore
UseOperatingSystemProfiles	Optional. Ermöglicht die Verwendung von Betriebssystemprofilen. Verwenden Sie diese Option, wenn der Integrationsdienst unter UNIX ausgeführt wird.
ValidateDataCodePages	Optional. Erzwingt Kompatibilität der Daten-Codepage. Der Standardwert lautet „Ja“.

Option	Beschreibung
WriterWaitTimeOut	<p>Optional. Dies ist im zielbasierten Commit-Modus die Zeit in Sekunden, während der der Writer inaktiv bleibt, bevor er eine Commit-Anweisung erteilt, wenn folgende Voraussetzungen zutreffen:</p> <ul style="list-style-type: none"> <li>- Der PowerCenter Integration Service hat Daten in das Target geschrieben.</li> <li>- Der PowerCenter Integration Service hat keine Commit-Anweisung erteilt.</li> </ul> <p>Der PowerCenter-Integrationsdienst kann dem Ziel vor oder nach dem konfigurierten Commit-Intervall eine Commit-Anweisung erteilen.</p> <p>Der Mindestwert lautet „60“. Der Maximalwert lautet 2592000. Der Standardwert lautet „60“.</p>
XMLWarnDupRows	<p>Optional. Schreibt Warnungen über duplizierte Zeilen und duplizierte Zeilen für XML-Ziele in das Sitzungsprotokoll. Der Standardwert lautet „Ja“.</p>

## Integration Service-Prozessoptionen

Geben Sie Dienstprozessoptionen im folgenden Format ein:

```
infacmd CreateIntegrationService ... -po option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Integration Service-Prozessoptionen beschrieben:

Option	Beschreibung
\$PMBadFileDir	<p>Optional. Standardverzeichnis für Ablehnungsdateien. Es darf die folgenden Sonderzeichen nicht enthalten:</p> <p>* ? &lt; &gt; "   ,</p> <p>Die Standardeinstellung ist \$PMRootDir/BadFiles.</p>
\$PMCacheDir	<p>Optional. Standardverzeichnis für Index- und Datencache-Dateien. Es darf die folgenden Sonderzeichen nicht enthalten:</p> <p>* ? &lt; &gt; "   ,</p> <p>Die Standardeinstellung ist \$PMRootDir/Cache.</p>
\$PMExtProcDir	<p>Optional. Standardverzeichnis für externe Prozeduren. Es darf die folgenden Sonderzeichen nicht enthalten:</p> <p>* ? &lt; &gt; "   ,</p> <p>Die Standardeinstellung ist \$PMRootDir/ExtProc.</p>
\$PMLookupFileDir	<p>Optional. Standardverzeichnis für Lookup-Dateien. Es darf die folgenden Sonderzeichen nicht enthalten:</p> <p>* ? &lt; &gt; "   ,</p> <p>Die Standardeinstellung ist \$PMRootDir/LkpFiles.</p>

Option	Beschreibung
\$PMRootDir	Optional. Root-Verzeichnis, auf das vom Knoten aus zugegriffen werden kann. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > "   , Die Standardeinstellung ist C:\Informatica\PowerCenter8.6\server\infa_shared.
\$PMSessionLogDir	Optional. Standardverzeichnis für Sitzungsprotokolle. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > "   , Die Standardeinstellung ist \$PMRootDir/SessLogs.
\$PMSourceFileDir	Optional. Standardverzeichnis für Quelldateien. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > "   , Die Standardeinstellung ist \$PMRootDir/SrcFiles.
\$PMStorageDir	Optional. Standardverzeichnis für Laufzeitdateien. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > "   , Die Standardeinstellung ist \$PMRootDir/Storage.
\$PMTargetFileDir	Optional. Standardverzeichnis für Target-Dateien. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > "   , Die Standardeinstellung ist \$PMRootDir/TgtFiles.
\$PMTempDir	Optional. Standardverzeichnis für temporäre Dateien. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > "   , Die Standardeinstellung ist \$PMRootDir/Temp.
\$PMWorkflowLogDir	Optional. Standardverzeichnis für Arbeitsablaufprotokolle. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > "   , Die Standardeinstellung ist \$PMRootDir/WorkflowLogs.
Codepage_ID	Erforderlich. ID-Nummer der Codepage für den Integration Service-Prozess.
JVMClassPath	Optional. Java SDK-Klassenpfad.
JVMMaxMemory	Optional. Der Maximalspeicher, den das Java SDK während einer PowerCenter-Sitzung verwendet. Der Standardwert beträgt 64 MB.
JVMMinMemory	Optional. Der Mindestspeicher, den das Java SDK während einer PowerCenter-Sitzung verwendet. Der Standardwert beträgt 32 MB.

# CreateMMService

Erstellt einen Metadata Manager-Dienst in der Domäne. Der Metadata Manager-Dienst wird standardmäßig deaktiviert, wenn Sie ihn erstellen. Führen Sie `infacmd EnableService` aus, um den Metadata Manager-Dienst zu aktivieren.

Der Befehl „`infacmd isp CreateMMService`“ verwendet die folgende Syntax:

```
CreateMMService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

<-ServiceOptions|-so> option_name=value ...>

[<-LicenseName|-ln> license_name]

[<-FolderPath|-fp> full_folder_path]
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd isp CreateMMService`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Metadata Manager-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht länger als 79 Zeichen sein und keine Leerzeichen, Wagenrückläufe, Tabulatoren oder die folgenden Zeichen enthalten:  / * ? < > "
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem die Metadata Manager-Anwendung ausgeführt werden soll.
-ServiceOptions -so	option_name=value	Optional. Diensteigenschaften, mit denen definiert wird, wie der Metadata Manager-Dienst ausgeführt wird.

Option	Argument	Beschreibung
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz, die Sie dem Metadata Manager-Dienst zuweisen möchten.
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, in dem Sie den Metadata Manager-Dienst erstellen möchten. Folgendes Format ist erforderlich:  <i>/parent_folder/child_folder</i>  Standardwert ist „/" (die Domäne).

## Metadata Manager-Dienst-Optionen

Geben Sie Metadata Manager-Dienst-Optionen im folgenden Format ein:

```
infacmd isp CreateMMService ... -so option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Metadata Manager-Dienst-Optionen beschrieben:

Option	Beschreibung
AgentPort	Erforderlich. Portnummer für den Metadata Manager Agent. Der Agent verwendet diesen Port zum Kommunizieren mit Metadaten-Quell-Repositorys. Standard ist 10251.
CodePage	Erforderlich. Codepage-Beschreibung für das Metadata Manager-Repository. Um eine Codepage einzugeben, die ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
ConnectionString	Erforderlich. Nativer Verbindungsstring für die Metadata Manager-Repository-Datenbank.
DBUser	Erforderlich. Benutzerkonto für die Metadata Manager-Repository-Datenbank.
DBPassword	Erforderlich. Passwort für den Metadata Manager-Repository-Datenbankbenutzer. Benutzerpasswort. Sie können ein Passwort mit der Option -so oder der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -so festgelegte Passwort Vorrang.
DatabaseHostname	Erforderlich. Hostname für die Metadata Manager-Repository-Datenbank.
DatabaseName	Erforderlich. Vollständiger Dienstname oder SID für Oracle-Datenbanken. Dienstname für IBM DB2-Datenbanken. Datenbankname für eine Microsoft SQL Server-Datenbank.
DatabasePort	Erforderlich. Portnummer für die Metadata Manager-Repository-Datenbank.
DatabaseType	Erforderlich. Typ der Datenbank für das Metadata Manager-Repository.

Option	Beschreibung
ErrorSeverityLevel	Optional. Level der in das Metadata Manager-Dienstprotokoll geschriebenen Fehlermeldungen Die Standardeinstellung ist ERROR.
FileLocation	Erforderlich. Speicherort der von der Metadata Manager-Anwendung verwendeten Dateien.
JdbcOptions	Optional. Weitere JDBC-Optionen. Sie können diese Eigenschaft verwenden, um die folgenden Informationen anzugeben: <ul style="list-style-type: none"> <li>- Speicherort des Sicherungsservers</li> <li>- Oracle ASO (Advanced Security Option)-Parameter</li> <li>- Microsoft SQL Server-Authentifizierungsparameter</li> <li>- Zusätzliche JDBC-Parameter bei Aktivierung der sicheren Kommunikation für die Metadata Manager-Repository-Datenbank</li> </ul> Weitere Informationen zu diesen Parametern finden Sie im <i>Handbuch für Informatica-Anwendungsdienste</i> .
MaxConcurrentRequests	Optional. Maximale Anzahl von Anfragen für die Verarbeitung verfügbarer Threads, die die maximale Anzahl der Clients-Anfragen bestimmt, die der Metadata Manager gleichzeitig bearbeiten kann. Standardwert ist 100.
MaxHeapSize	Optional. Dem JVM (Java Virtual Manager), auf dem Metadata Manager ausgeführt wird, zugeordnete RAM-Größe (in MB). Standard ist 512.
MaxQueueLength	Optional. Maximale Warteschlangenlänge für eingehende Verbindungsanfragen, wenn alle möglichen Anfragen verarbeitende Threads von der Metadata Manager-Anwendung genutzt werden Standardwert ist 500.
MaximumActiveConnections	Optional. Anzahl der für die Metadata Manager-Repository-Datenbank verfügbaren aktiven Verbindungen. Die Metadata Manager-Anwendung unterhält einen Verbindungspool für die Verbindung zur Repository-Datenbank. Standard ist 20.
MaximumWaitTime	Optional. Max. Zeitraum (in Sekunden), für den der Metadata Manager die Datenbank-Verbindungsanfragen im Verbindungspool speichert Standardwert ist „180“.
MetadataTreeMaxFolderChilds	Optional. Anzahl der untergeordneten Objekte, die im Metadata Manager-Metadatenkatalog für alle übergeordneten Objekte angezeigt werden Standardwert ist 100.
ODBCConnectionMode	Vom Integrationsdienst verwendeter Verbindungsmodus, um eine Verbindung zu Metadatenquellen und dem Metadata Manager-Repository beim Laden von Ressourcen herzustellen. Der Wert kann TRUE oder FALSE sein.  Sie müssen diese Eigenschaft auf „true“ festlegen, wenn der Integrationsdienst auf einem UNIX-Computer ausgeführt wird und Sie Metadaten aus einer Microsoft SQL Server-Datenbank laden möchten oder wenn Sie eine Microsoft SQL Server-Datenbank für das Metadata Manager-Repository verwenden.
OracleConnType	Erforderlich, wenn Sie Oracle als DatabaseType auswählen. Oracle-Verbindungstyp. Sie können eine der folgenden Optionen eingeben: <ul style="list-style-type: none"> <li>- OracleSID</li> <li>- OracleServiceName</li> </ul>
PortNumber	Erforderlich. Portnummer, auf der die Metadata Manager-Anwendung ausgeführt wird. Standard ist 10250.



Option	Beschreibung
StagePoolSize	Optional. Maximale Anzahl der Ressourcen, die vom Metadata Manager gleichzeitig geladen werden Standard ist 3.
TablespaceName	Tablespace-Name für das Metadata Manager-Repository unter IBM DB2.
TimeoutInterval	Optional. Zeitraum in Minuten, in dem der Metadata Manager eine fehlgeschlagene Ressourcenlast in der Ladewarteschlange speichert. Standard ist 30.
URLScheme	Erforderlich. Gibt das Sicherheitsprotokoll an, das Sie für die Metadata Manager-Anwendung konfigurieren: HTTP oder HTTPS.
keystoreFile	Erforderlich, wenn Sie HTTPS verwenden. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die bei Verwendung des SSL-Sicherheitsprotokolls mit der Metadata Manager-Anwendung erforderlich sind.

## CreateOSProfile

Erstellt ein Betriebssystemprofil in der Domäne. Bevor Sie Arbeitsabläufe ausführen, die Betriebssystemprofile verwenden, müssen Sie den PowerCenter-Integrationsdienst zur Verwendung von Betriebssystemprofilen konfigurieren.

Der Befehl „infacmd isp CreateOSProfile“ verwendet die folgende Syntax:

```
CreateOSProfile
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-OSProfileName|-on> OSProfile_name
<-SystemName|-sn> system_username
[<-IntegrationServiceProcessOptions|-po> option_name=value ...]
[<-EnvironmentVariables|-ev> name=value ...]
[<-DISProcessVariables|-diso> option_name=value ...]
[<-DISEnvironmentVariables|-dise> name=value ...]
[<-HadoopImpersonationProperties|-hipr> hadoop_impersonation_properties]
[<-HadoopImpersonationUser|-hu> hadoop_impersonation_user]
[<-UseLoggedInUserAsProxy|-ip> use_logged_in_user_as_proxy]
[<-ProductExtensionName|-pe> product_extension_name]
[<-ProductOptions|-o> optionGroupName.optionName=Value ...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateOSProfile“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-OSProfileName -on	OSProfile_name	Erforderlich. Name des Betriebssystemprofils. Der Name des Betriebssystemprofils kann bis zu 80 Zeichen enthalten. Er darf weder Leerzeichen noch die folgenden Sonderzeichen enthalten:  % * + \ / ? ; < >
-SystemName -sn	system_username	Erforderlich. Name eines Betriebssystembenutzers, der auf den Computern vorhanden ist, auf denen der Integrationsdienst ausgeführt wird. Der Integrationsdienst führt Arbeitsabläufe mit dem Systemzugriff desjenigen Systembenutzers aus, der für das Betriebssystemprofil definiert wurde.
- IntegrationServiceProcessOptions -po	option_name=value	Optional. Dienstprozeßeigenschaften, mit denen definiert wird, wie der PowerCenter-Integrationsdienst ausgeführt wird.
-EnvironmentVariables -ev	name=value	Optional. Name und Wert von Umgebungsvariablen, die vom PowerCenter-Integrationsdienst zur Laufzeit verwendet werden.
-DISProcessVariables -diso	option_name=value	Optional. Dienstprozeßeigenschaften, mit denen definiert wird, wie der Datenintegrationsdienst ausgeführt wird.
-DISEnvironmentVariables -dise	name=value	Optional. Name und Wert von Umgebungsvariablen, die vom Datenintegrationsdienst zur Laufzeit verwendet werden.
-HadoopImpersonationProperties -hipr	hadoop_impersonation_properties	Optional. Gibt an, ob der Datenintegrationsdienst den Hadoop-Identitätswechselbenutzer zum Ausführen von Mappings, Arbeitsabläufen und Profiling-Aufträgen in einer Hadoop-Umgebung verwendet. Gültige Werte sind „True“ oder „False“.
-HadoopImpersonationUser -hu	hadoop_impersonation_user	Optional. Geben Sie einen Benutzernamen für den Datenintegrationsdienst zum Identitätswechsel an, wenn er einen Auftrag in einer Hadoop-Umgebung ausführt.
-UseLoggedInUserAsProxy -ip	use_logged_in_user_as_proxy	Optional. Gibt an, ob der angemeldete Benutzer als Hadoop-Identitätswechselbenutzer verwendet werden soll. Gültige Werte sind „True“ oder „False“.

Option	Argument	Beschreibung
-ProductExtensionName -pe	product_extension_name	Optional. Für zukünftige Verwendung reserviert.
-ProductOptions -o	optionGroupName.optionName=Value	<p>Erforderlich. Name und Wert jeder von Ihnen festgelegten Option. Erstellen Sie mit dieser Option ein Cache-Verzeichnis für Einfachdateien, das vom Betriebssystemprofil verwendet werden kann.</p> <p>Mit dem folgenden Befehl wird das Cache-Verzeichnis beispielsweise auf „\$PMRootDir/OSPCache“ festgelegt:</p> <pre>infacmd isp createOSProfile ... -o 'runTimeVariables.flatFileCacheDirectory'=" \$PMRootDir/OSPCache"</pre>

## Datenintegrationsdienst-Prozessoptionen für Betriebssystemprofile

Geben Sie die Prozessoptionen des Datenintegrationsdiensts in folgendem Format ein:

```
infacmd CreateOSProfile ... -diso option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Prozessoptionen des Datenintegrationsdiensts beschrieben:

Option	Beschreibung
\$DISRootDir	<p>Root-Verzeichnis, auf das vom Knoten aus zugegriffen werden kann. Dies ist das Root-Verzeichnis für andere Dienstprozessvariablen. Es darf keines der folgenden Sonderzeichen enthalten sein:</p> <p>* ? &lt; &gt; "   , [ ]</p>
\$DISTempDir	<p>Verzeichnis für temporäre Dateien, die während der Ausführung von Jobs erstellt werden. Es darf keines der folgenden Sonderzeichen enthalten sein:</p> <p>* ? &lt; &gt; "   , [ ]</p> <p>Standardwert ist &lt;Root-Verzeichnis&gt;/disTemp.</p> <p><b>Hinweis:</b> Wenn der Datenintegrationsdienst für die Verwendung mehrerer Betriebssystemprofile konfiguriert ist, geben Sie ein gemeinsames Verzeichnis für alle Profile an, da ein separates Verzeichnis für jedes Profil zu einer übermäßigen Nutzung des Speicherplatzes führt.</p>
\$DISCacheDir	<p>Verzeichnis für Index- und Daten-Cache-Dateien für Umwandlungen. Es darf keines der folgenden Sonderzeichen enthalten sein:</p> <p>* ? &lt; &gt; "   , [ ]</p> <p>Standardwert ist &lt;Root-Verzeichnis&gt;/cache.</p>
\$DISSourceDir	<p>Verzeichnis für Einfachdateien der Quelle, die in einem Mapping verwendet werden. Es darf keines der folgenden Sonderzeichen enthalten sein:</p> <p>* ? &lt; &gt; "   , [ ]</p> <p>Standardwert ist &lt;Root-Verzeichnis&gt;/source.</p>

Option	Beschreibung
\$DISTargetDir	Verzeichnis für Einfachdateien des Ziels, die in einem Mapping verwendet werden. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > "   , [ ] Standardwert ist <Root-Verzeichnis>/target.
\$DISRejectedFilesDir	Verzeichnis für Ablehnungsdateien. Ablehnungsdateien enthalten Zeilen, die beim Ausführen eines Mappings zurückgewiesen wurden. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > "   , [ ] Standardwert ist <Root-Verzeichnis>/reject.
\$DISLogDir	Verzeichnis für Protokolle. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > "   , [ ] Standardwert ist <Root-Verzeichnis>/disLogs.

## PowerCenter-Integrationsdienst-Prozessoptionen für Betriebssystemprofile

Geben Sie die Prozessoptionen des PowerCenter-Integrationsdiensts in folgendem Format ein:

```
infacmd CreateOSProfile ... -po option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Prozessoptionen des PowerCenter-Integrationsdiensts beschrieben:

Option	Beschreibung
\$PMBadFileDir	Optional. Verzeichnis für Ablehnungsdateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > "   , Standardwert ist \$PMRootDir/BadFiles.
\$PMCacheDir	Optional. Verzeichnis für Index- und Datencache-Dateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > "   , Standardwert ist \$PMRootDir/Cache.
\$PMExtProcDir	Optional. Verzeichnis für externe Prozeduren. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > "   , Standardwert ist \$PMRootDir/ExtProc.
\$PMLookupFileDir	Optional. Verzeichnis für Lookup-Dateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > "   , Standardwert ist \$PMRootDir/LkpFiles.

Option	Beschreibung
\$PMRootDir	Optional. Root-Verzeichnis, auf das vom Knoten aus zugegriffen werden kann. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > "   , Standardwert ist C:\Informatica\PowerCenter\server\infa_shared.
\$PMSessionLogDir	Optional. Verzeichnis für Sitzungsprotokolle. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > "   , Standardwert ist \$PMRootDir/SessLogs.
\$PMSourceFileDir	Optional. Verzeichnis für Quelldateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > "   , Standardwert ist \$PMRootDir/SrcFiles.
\$PMStorageDir	Optional. Verzeichnis für Laufzeitdateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > "   , Standardwert ist \$PMRootDir/Storage.
\$PMTargetFileDir	Optional. Verzeichnis für Zieldateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > "   , Standardwert ist \$PMRootDir/TgtFiles.
\$PMTempDir	Optional. Verzeichnis für temporäre Dateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > "   , Standardwert ist \$PMRootDir/Temp.

## CreateRepositoryService

Erstellt einen PowerCenter-Repository-Dienst in einer Domäne.

Der PowerCenter-Repository-Dienst wird standardmäßig bei seiner Erstellung aktiviert.

Ein PowerCenter-Repository-Dienst verwaltet ein Repository. Er führt alle Metadatentransaktionen zwischen dem Repository und Repository-Clients aus.

Der Befehl „infacmd isp CreateRepositoryService“ verwendet die folgende Syntax:

```
CreateRepositoryService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

[<-BackupNodes|-bn> node1 node2 ...]

[<-ServiceDisable|-sd>]

<-ServiceOptions|-so> option_name=value ...

[<-LicenseName|-ln> license_name]

[<-FolderPath|-fp> full_folder_path]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateRepositoryService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des PowerCenter-Repository-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten:  \ / : * ? < > "
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der PowerCenter-Repository-Dienstprozess ausgeführt werden soll. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, gibt diese Option den Namen des primären Knotens an.
-BackupNodes -bn	node1 node2 ...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Sicherungsknoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.
-ServiceDisable -sd	-	Optional. Erstellt einen deaktivierten Dienst. Sie müssen den Dienst aktivieren, bevor Sie ihn ausführen können.
-ServiceOptions -so	option_name=value	Erforderlich. Diensteseigenschaften, mit denen definiert wird, wie der PowerCenter-Repository-Dienst ausgeführt wird.
-LicenseName -ln	license_name	Erforderlich, wenn Sie einen aktivierten Dienst erstellen. Name der Lizenz, die Sie dem PowerCenter-Repository-Dienst zuweisen möchten.
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, in dem Sie den PowerCenter-Repository-Dienst erstellen möchten. Folgendes Format ist erforderlich:  <i>/parent_folder/child_folder</i>  Standardwert ist „/“ (die Domäne).

## Repository-Dienst-Optionen (-so)

Geben Sie Repository-Dienst-Optionen im folgenden Format ein:

```
infacmd CreateRepositoryService ... -so option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.



In der folgenden Tabelle werden die Repository-Dienst-Optionen beschrieben:

Option	Beschreibung
AllowWritesWithRACaching	Optional. Verwendet PowerCenter Client-Tools zum Ändern von Metadaten im Repository, wenn „RepAgent cachern“ aktiviert ist. Standardwert ist „Ja“.
CheckinCommentsRequired	Optional. Beim Einchecken von Repository-Objekten müssen Benutzer Kommentare hinzufügen. Standardwert ist „Ja“. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
CodePage	Erforderlich. Codepage-Beschreibung für die Datenbank. Zur Eingabe einer Codepage, die ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
ConnectionString	Erforderlich. Die während der Einrichtung des PowerCenter-Repository-Diensts angegebene Datenbankverbindungszeichenfolge. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
DBPassword	Erforderlich. Repository-Datenbankpasswort für den Datenbankbenutzer. Sie können ein Passwort mit der Option -so oder der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -so festgelegte Passwort Vorrang. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
DBPoolExpiryThreshold	Optional. Die Mindestanzahl an inaktiven Datenbankverbindungen, die im PowerCenter-Repository-Dienst zulässig sind. Beispiel: Wenn 20 inaktive Verbindungen vorhanden sind und Sie diesen Schwellenwert auf 5 festlegen, schließt der PowerCenter-Repository-Dienst höchstens 15 Verbindungen. Die Mindestanzahl beträgt 3. Standardwert ist 5.
DBPoolExpiryTimeout	Optional. Der Zeitraum in Sekunden, in dem der PowerCenter-Repository-Dienst nach inaktiven Datenbankverbindungen sucht. Ist eine Verbindung für einen Zeitraum inaktiv, der diesen Wert überschreitet, kann der PowerCenter-Repository-Dienst die Verbindung schließen. Der Mindestwert beträgt 300. Der Höchstwert beträgt 2.592.000 (30 Tage). Standardwert ist 3.600 (1 Stunde).
DBUser	Erforderlich. Konto für die Datenbank, die das Repository enthält. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
DatabaseArrayOperationSize	Optional. Anzahl der Zeilen, die bei jedem Array-Datenbankvorgang abgerufen werden, beispielsweise Einfügen oder Abrufen. Standardwert ist 100. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
DatabaseConnectionTimeout	Optional. Zeitraum in Sekunden, in dem der PowerCenter-Repository-Dienst versucht, eine Verbindung zum Datenbankverwaltungssystem herzustellen. Standardwert ist 180.
DatabasePoolSize	Optional. Maximale Anzahl der Verbindungen zur Repository-Datenbank, die der PowerCenter-Repository-Dienst herstellen kann. Der Mindestwert beträgt 20. Standardwert ist 500.
DatabaseType	Erforderlich. Typ der Datenbank, die die Repository-Metadaten speichert. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
EnableRepAgentCaching	Optional. Aktiviert die Funktion „Repository Agent Caching“. Standardwert ist „Ja“.

Option	Beschreibung
ErrorSeverityLevel	Optional. Mindestebene der Fehlermeldungen, die in das PowerCenter-Repository-Dienstprotokoll geschrieben werden: <ul style="list-style-type: none"> <li>- Fatal</li> <li>- Fehler Warnung</li> <li>- Info</li> <li>- Trace</li> <li>- Debug</li> </ul> Der Standardwert lautet „Info“.
HeartBeatInterval	Optional. Zeitraum, in dem der PowerCenter-Repository-Dienst seine Verbindungen zu den Clients in diesem Dienst überprüft. Standardwert ist 60 Sekunden.
MaxResilienceTimeout	Optional. Maximaler Zeitraum in Sekunden, in dem der Dienst die Ressourcen zwecks Belastbarkeit beibehält. Standardwert ist 180.
MaximumConnections	Optional. Maximale Anzahl der Verbindungen, die das Repository von den Repository-Clients akzeptiert. Standardwert ist 200.
MaximumLocks	Optional. Maximale Anzahl an Sperren, die das Repository für Metadatenobjekte verwendet. Standardwert ist 50.000.
OperatingMode	Optional. Modus, in dem der PowerCenter-Repository-Dienst ausgeführt wird: <ul style="list-style-type: none"> <li>- Normal</li> <li>- Exklusiv</li> </ul> Standardwert ist „Normal“. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
OptimizeDatabaseSchema	Optional. Optimiert das Repository-Datenbankschema beim Erstellen von Repository-Inhalten oder Sichern und Wiederherstellen eines IBM DB2- oder Microsoft SQL Server-Repositorys. Bei Aktivierung versucht der PowerCenter-Repository-Dienst Repository-Tabellen zu erstellen, die Varchar-Spalten mit einer Genauigkeit von 2000 anstelle von CLOB-Spalten enthalten. Verwenden Sie Varchar-Spalten, um die Leistung des Repositorys zu steigern. Bei Verwendung von Varchar-Spalten verringern Sie die Festplatteneingabe und -ausgabe und die Datenbank kann die Spalten zwischenspeichern. <p>Um diese Option zu verwenden, überprüfen Sie die Anforderungen an die Seitengröße für die folgenden Repository-Datenbanken:</p> <ul style="list-style-type: none"> <li>- IBM DB2. Datenbank-Seitengröße 4 KB oder größer. Mindestens einen temporären Tablespace mit einer Seitengröße von mindestens 16 KB.</li> <li>- Microsoft SQL Server. Datenbank-Seitengröße 8 KB oder größer.</li> </ul> Standardwert ist „Deaktiviert“.
PreserveMXData	Optional. Behält MX-Daten für frühere Versionen von Zuordnungen bei. Standardwert ist „Deaktiviert“.
RACacheCapacity	Optional. Anzahl der Objekte, die der Cache bei aktiviertem Repository Agent Caching enthalten kann. Standardwert ist 10.000.
SecurityAuditTrail	Optional. Verfolgt Änderungen, die an Benutzern, Gruppen und Berechtigungen vorgenommen wurden. Standardwert ist „Nein“.

Option	Beschreibung
ServiceResilienceTimeout	Optional. Zeitraum in Sekunden, in dem der Dienst versucht, eine Verbindung zu einem anderen Dienst herzustellen oder erneut herzustellen. Standardwert ist 180. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
TableOwnerName	Optional. Name des Eigentümers der Repository-Tabellen für ein IBM DB2-Repository.
TablespaceName	Optional. Tablespace-Name für IBM DB2-Repositorys. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
TrustedConnection	Optional. Verwendet Windows-Authentifizierung, um auf die Microsoft SQL Server-Datenbank zuzugreifen. Standardwert ist „Nein“. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.

## CreateRole

Erstellt eine benutzerdefinierte Rolle in der Domäne. Anschließend können Sie der Rolle Berechtigungen für die Domäne oder für einen Anwendungsdiensttyp zuweisen. Sie können keine systemdefinierten Rollen erstellen.

Der Befehl „infacmd isp CreateRole“ verwendet die folgende Syntax:

```
CreateRole
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
[<-SecurityDomain|-sdn> securitydomain]
<-Password|-pd> password
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-RoleName|-rn> role_name
[<-RoleDescription|-rd> role_description]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateRole“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-RoleName -rn	role_name	<p>Erforderlich. Name der Rolle. Der Rollenname unterliegt nicht der Groß-/Kleinschreibung und kann 1 bis 80 Zeichen umfassen. Er darf weder Tabulatoren, Zeilenendzeichen noch folgende Sonderzeichen enthalten:</p> <p>, + " \ &lt; &gt; ; / * % ?</p> <p>Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Alle anderen Leerzeichen sind nicht zulässig.</p>
-RoleDescription -rd	role_description	<p>Optional. Rollenbeschreibung. Die Beschreibung kann maximal 1.000 Zeichen umfassen und darf weder Tabulatoren, Zeilenendzeichen noch folgende Sonderzeichen enthalten:</p> <p>&lt; &gt; "</p> <p>Um eine Beschreibung einzugeben, die Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen.</p>

## CreateSAPBWService

Erstellt einen SAP BW-Dienst in der Domäne. Der SAP BW-Dienst wird standardmäßig aktiviert, wenn Sie ihn erstellen.

Der Befehl „infacmd isp CreateSAPBWService“ verwendet die folgende Syntax:

```
CreateSAPBWService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

<-IntegrationService|-is> integration_service_name

<-RepositoryUser|-ru> user

<-RepositoryPassword|-rp> password

[<-ServiceOptions|-so> option_name=value ...]

[<-ServiceProcessOptions|-po> option_name=value ...]

[<-ServiceDisable|-sd>]

[<-LicenseName|-ln> license_name]
```

```
[<-FolderPath|-fp> full_folder_path]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateSAPBWService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des SAP BW-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten:  / * ? < > "
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der SAP BW-Dienst-Prozess ausgeführt werden soll. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, gibt diese Option den Namen des primären Knotens an.
-IntegrationService -is	integration_service_name	Erforderlich. Name des Integrationsdiensts, zu dem der SAP BW-Dienst eine Verbindung herstellt. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryUser -ru	user	Erforderlich. Benutzername zum Herstellen einer Verbindung zum Repository. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryPassword -rp	Passwort	Erforderlich, wenn die sichere Kommunikation nicht für die Domäne aktiviert ist. Optional, wenn die sichere Kommunikation für die Domäne aktiviert ist. Benutzerpasswort. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -rp festgelegte Passwort Vorrang.
-ServiceOptions -so	option_name=value	Optional. Diensteigenschaften, mit denen definiert wird, wie der SAP BW-Dienst ausgeführt wird.
-ServiceProcessOptions -po	option_name=value	Optional. Dienstprozesseigenschaften für den SAP BW-Dienst.
-ServiceDisable -sd	-	Optional. Erstellt einen deaktivierten Dienst. Sie müssen den Dienst aktivieren, bevor Sie ihn ausführen können.

Option	Argument	Beschreibung
-LicenseName -ln	license_name	Erforderlich, wenn Sie einen aktivierten Dienst erstellen. Name der Lizenz, die Sie dem SAP BW-Dienst zuweisen möchten.
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, in dem Sie den SAP BW-Dienst erstellen möchten. Folgendes Format ist erforderlich:  <i>/parent_folder/child_folder</i> Standardwert ist „/“ (die Domäne).

## SAP BW Service-Optionen

Geben Sie SAP BW Service-Optionen im folgenden Format ein:

```
infacmd CreateSAPBWService ... -so option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die SAP BW Service-Optionen beschrieben:

Option	Beschreibung
BWSystemConxString	Optional. In der Datei <i>sapnwrfc.ini</i> definierter DEST-Eintrag für eine Verbindung zu einem RFC-Serverprogramm. Bearbeiten Sie diese Eigenschaft, wenn Sie in der Datei <i>sapnwrfc.ini</i> einen anderen DEST-Eintrag für den SAP BW-Dienst erstellt haben.
RetryPeriod	Optional. Anzahl der Sekunden, die der SAP BW Service wartet, bevor er eine Verbindung zum BW-System herstellt, wenn ein vorheriger Verbindungsversuch fehlgeschlagen ist. Standardwert ist „5“.

## SAP BW Service-Prozessoption

Geben Sie die Dienstprozessoptionen im folgenden Format ein:

```
infacmd CreateSAPBWService ... -po option_name=value
```

Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle wird die SAP BW Service-Option beschrieben:

Option	Beschreibung
ParamFileDir	Optional. Temporäres Verzeichnis für Parameterdateien. Standardverzeichnis ist <i>/Infa_Home/server/inf_a_shared/BWParam</i> .



# CreateUser

Erstellt ein Benutzerkonto in der nativen Sicherheitsdomäne. Anschließend können Sie Rollen und Berechtigungen zu einem Benutzerkonto zuweisen. Die einem Benutzer zugewiesenen Rollen und Berechtigungen legen die Aufgaben fest, die der Benutzer innerhalb der Domäne durchführen kann.

Der Befehl „infacmd isp CreateUser“ verwendet die folgende Syntax:

```
CreateUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NewUserName|-nu> new_user_name

<-NewUserPassword|-np> new_user_password

[<-NewUserFullName|-nf> new_user_full_name]

[<-NewUserDescription|-ds> new_user_description]

[<-NewUserEmailAddress|-em> new_user_email_address]

[<-NewUserPhoneNumber|-pn> new_user_phone_number]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NewUserName -nu	new_user_name	Erforderlich. Anmeldename für das Benutzerkonto. Der Anmeldename für ein Benutzerkonto muss innerhalb der Sicherheitsdomäne, zu der er gehört, eindeutig sein.  Der Anmeldename unterliegt nicht der Groß-/Kleinschreibung und kann 1 bis 80 Zeichen umfassen. Er darf weder Tabulatoren, Zeilenendzeichen noch folgende Sonderzeichen enthalten:  , + " \ < > ; / * & % ?  Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Alle anderen Leerzeichen sind nicht zulässig.

Option	Argument	Beschreibung
-NewUserPassword -np	new_user_password	<p>Erforderlich. Passwort für das Benutzerkonto. Sie können ein Passwort mit der Option -np oder der Umgebungsvariable INFA_PASSWORD festlegen. Wenn Sie ein Passwort mit diesen beiden Methoden festlegen, hat das mit der Option -np festgelegte Passwort Vorrang.</p> <p>Wenn Sie für ein natives Benutzerkonto die Passwortkomplexität aktivieren, beachten Sie beim Erstellen oder Ändern eines Passworts Folgendes:</p> <ul style="list-style-type: none"> <li>- Das Passwort muss aus mindestens acht Zeichen bestehen.</li> <li>- Es muss mindestens einen Buchstaben, eine Zahl und ein nicht alphanumerisches Zeichen enthalten, z. B.:  ! \ " # \$ % &amp; ' ( ) * + , - . / : ; &lt; = &gt; ? @  [ ] ^ _ ` {   } ~</li> </ul> <p>Manche Sonderzeichen in Passwörtern können von der Shell anders interpretiert werden. Beispielsweise wird \$ als Variable interpretiert. Setzen Sie in diesem Fall ein Escape-Zeichen vor das betreffende Sonderzeichen.</p>
-NewUserFullName -nf	new_user_full_name	<p>Optional. Vollständiger Name für das Benutzerkonto. Um einen Namen einzugeben, der Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen. Der vollständige Name darf folgende Sonderzeichen nicht enthalten:</p> <p>&lt; &gt; \"</p>
-NewUserDescription -ds	new_user_description	<p>Optional. Beschreibung des Benutzerkontos. Um eine Beschreibung einzugeben, die Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen.</p> <p>Die Beschreibung darf die folgenden Sonderzeichen nicht enthalten:</p> <p>&lt; &gt; \"</p>
-NewUserEmailAddress -em	new_user_email_address	<p>Optional. E-Mail-Adresse des Benutzers. Um eine Adresse einzugeben, die Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen.</p> <p>Die E-Mail-Adresse darf keines der folgenden Sonderzeichen enthalten:</p> <p>&lt; &gt; \"</p> <p>Geben Sie die E-Mail-Adresse im Format UserName@Domain ein.</p>
-NewUserPhoneNumber -pn	new_user_phone_number	<p>Optional. Telefonnummer des Benutzers. Um eine Telefonnummer einzugeben, die Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen.</p> <p>Die Telefonnummer darf keines der folgenden Sonderzeichen enthalten:</p> <p>&lt; &gt; \"</p>

# CreateWSHubService

Erstellt einen Webdienst-Hub in der Domäne. Der Webdienst-Hub wird standardmäßig aktiviert, wenn Sie ihn erstellen.

Der Befehl „infacmd isp CreateWSHubService“ verwendet die folgende Syntax:

```
CreateWSHubService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
[<-FolderPath|-fp> full_folder_path]
<-NodeName|-nn> node_name
<-RepositoryService|-rs> repository_service_name
<-RepositoryUser|-ru> repository_user
<-RepositoryPassword|-rp> repository_password
[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]
[<-ServiceDisable|-sd>]
[<-ServiceOptions|-so> option_name=value ...]
<-LicenseName|-ln> license_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateWSHubService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Domäne.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Name des Webdienst-Hubs, den Sie erstellen möchten. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten:  <code>/ * ? &lt; &gt; "  </code>
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, in dem Sie den Webdienst-Hub erstellen möchten. Folgendes Format ist erforderlich:  <code>/parent_folder/child_folder</code> Standardwert ist „/“ (die Domäne).
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Webdienst-Hub-Prozess ausgeführt werden soll.

Option	Argument	Beschreibung
-RepositoryService -rs	repository_service_name	Erforderlich. Name des Repository-Diensts, von dem der Webdienst-Hub abhängig ist.  Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryUser -ru	repository_user	Erforderlich. Benutzername zum Herstellen einer Verbindung zum Repository.  Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryPassword -rp	repository_password	Erforderlich. Benutzerpasswort. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-rp“ festgelegte Passwort Vorrang.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung oder Kerberos-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der PowerCenter-Repository-Benutzer gehört.  Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ServiceDisable -sd	-	Optional. Erstellt einen deaktivierten Dienst. Sie müssen den Dienst aktivieren, bevor Sie ihn ausführen können.
-ServiceOptions -so	option_name=value ...	Optional. Diensteigenschaften, mit denen definiert wird, wie der Webdienst-Hub ausgeführt wird.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz, die Sie dem Webdienst-Hub zuweisen möchten.

## Web Services Hub-Optionen

Geben Sie Web Services Hub-Optionen im folgenden Format ein:

```
infacmd CreateWSHubService ... -so option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden Web Services Hub-Optionen beschrieben:

Option	Beschreibung
DTMTimeout	Optional. Zeit in Sekunden, in der <i>infacmd</i> versucht, eine Verbindung zu DTM herzustellen bzw. erneut herzustellen. Default is 60.
ErrorSeverityLevel	Optional. Mindestlevel der Fehlerprotokollierung für die Web Services Hub-Protokolle: <ul style="list-style-type: none"> <li>- Schwerwiegend</li> <li>- Fehler</li> <li>- Warnung</li> <li>- Info</li> <li>- Trace</li> <li>- Debug</li> </ul> Die Standardeinstellung lautet "Info".
HubHostName	Optional. Name des Computers, auf dem der Web Services Hub gehostet wird. Der Standardwert ist "localhost". Um die Änderungen zu übernehmen, starten Sie den Web Services Hub neu.
HubPortNumber(http)	Optional. Portnummer, auf der der Web Services Hub in Tomcat ausgeführt wird. Default is 7333. Um die Änderungen zu übernehmen, starten Sie den Web Services Hub neu.
HubPortNumber (https)	Portnummer, auf der der Web Services Hub in Tomcat ausgeführt wird. Erforderlich, wenn Sie den Web Services Hub unter HTTPS ausführen möchten. Default is 7343.
InternalHostName	Optional. Hostname, mit dem der Web Services Hub Verbindungen vom Integration Service abhört. Der Standardwert ist "localhost". Um die Änderungen zu übernehmen, starten Sie den Web Services Hub neu.
InternalPortNumber	Optional. Portnummer, mit der der Web Services Hub Verbindungen vom Integration Service abhört. Default is 15555. Um die Änderungen zu übernehmen, starten Sie den Web Services Hub neu.
MaxConcurrentRequests	Optional. Maximale Anzahl an verfügbaren Verarbeitungs-Threads, mit der die maximale Anzahl an gleichzeitigen Anfragen, die verarbeitet werden können, angegeben wird. Default is 100.
MaxLMConnections	Optional. Maximale Anzahl an Verbindungen zum Integration Service, die für den Web Services Hub gleichzeitig offen sein können. Default is 20.
MaxQueueLength	Optional. Maximale Warteschlangenlänge für eingehende Verbindungsanfragen, wenn alle möglichen Threads für die Verarbeitung von Anfragen verwendet werden. Default is 5000.
SessionExpiryPeriod	Optional. Anzahl an Sekunden, die eine Sitzung ungenutzt bleiben kann, bevor ihre Sitzungs-ID ungültig wird. Die Standardeinstellung lautet 3600 Sekunden.
URLScheme	Optional. Das von Ihnen konfigurierte Sicherheitsprotokoll für den Web Services Hub: HTTP oder HTTPS. Standardwert ist HTTP. Um die Änderungen zu übernehmen, starten Sie den Web Services Hub neu.

Option	Beschreibung
WSH_ENCODING	Optional. Zeichenkodierung für den Web Services Hub. Standardmäßig wird UTF-16LE verwendet. Um die Änderungen zu übernehmen, starten Sie den Web Services Hub neu.
KeystoreFile	Optional. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die für die Verwendung des SSL-Sicherheitsprotokolls mit dem Web Services Hub erforderlich sind.

## DeleteNamespace

Löscht eine LDAP-Sicherheitsdomäne und die Benutzer und Gruppen in der Sicherheitsdomäne. Löscht die LDAP-Sicherheitsdomäne, wenn die Informatica-Domäne LDAP oder die Kerberos-Authentifizierung verwendet.

Der Befehl „infacmd isp DeleteNamespace“ verwendet die folgende Syntax:

```

DeleteNamespace

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NameSpace|-ns> namespace

```



In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp DeleteNamespace“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, die Sie erstellen möchten und zu dem Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Sie können einen Wert für -sdn angeben oder den Standardwert basierend auf dem Authentifizierungsmodus verwenden: <ul style="list-style-type: none"> <li>- Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Standardwert ist „Native“. Zum Arbeiten mit der LDAP-Authentifizierung müssen Sie den Wert für -sdn angeben.</li> <li>- Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Standardwert ist „Native“ für native Authentifizierung. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</li> </ul>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn Sie die Umgebungsvariable nicht angeben, wird der Standardwert von 180 Sekunden verwendet.
-NameSpace -ns	namespace	Erforderlich. Name der LDAP- oder Kerberos-Sicherheitsdomäne. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf weder Leerzeichen noch folgende Sonderzeichen enthalten: , + / < > @ ; \ % ? Der Name darf nicht länger als 128 Zeichen sein. Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Sie können keine anderen Leerzeichen verwenden.

## DisableNodeResource

Deaktiviert eine Informatica-Ressource. Informatica-Ressourcen beinhalten Datei-Verzeichnisressourcen, benutzerspezifische Ressourcen und Verbindungsressourcen. Deaktivieren Sie die Ressourcen, die nicht verfügbar sind, um zu verhindern, dass der Load Balancer eine Aufgabe an einen Knoten sendet, der nicht über die erforderlichen Ressourcen verfügt.

Sie können Dateiverzeichnisressourcen, benutzerspezifische Ressourcen und Verbindungsressourcen deaktivieren.

Wenn ein PowerCenter-Integrationsdienst in einem Gitter ausgeführt wird, kann der Load Balancer Ressourcen verwenden, um Sitzungs-, Befehls- und vordefinierte Event-Wait-Aufgaben zu verteilen. Wenn der PowerCenter-Integrationsdienst für die Überprüfung von Ressourcen konfiguriert ist, verteilt der Load Balancer Aufgaben an Knoten mit verfügbaren Ressourcen.

Standardmäßig werden alle Verbindungsressourcen auf einem Knoten aktiviert.

Der Befehl „infacmd isp DisableNodeResource“ verwendet die folgende Syntax:

```
DisableNodeResource

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

[<-ResourceCategory|-rc> resource_category ("PCIS", "DIS")]

<-ResourceType|-rt> resource_type ("Custom", "File Directory", "Connection")
```

<-ResourceName|-rn> resource\_name

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp DisableNodeResource“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem die Ressource definiert ist.
-ResourceCategory -rc	resource_category	Optional. Kategorie der Ressource. Gültige Kategorien umfassen: - PCIS. Ressource für den PowerCenter-Integrationsdienst. - DIS. Für zukünftige Verwendung reserviert. Standardwert ist PCIS.
-ResourceType -rt	resource_type	Erforderlich. Typ der Ressource. Gültige Typen umfassen: - Benutzerdefiniert - Dateiverzeichnis - Verbindung
-ResourceName -rn	resource_name	Erforderlich. Vollständiger Name der Ressource. Um die Namen aller für einen Knoten verfügbaren Ressourcen aufzulisten, führen Sie den infacmd isp ListNodeResources-Befehl aus.

## DisableService

Deaktiviert den Anwendungsdienst, der dem Dienstnamen entspricht. Wenn Sie einen Dienst deaktivieren, werden alle Dienstprozesse gestoppt.

Deaktiviert jeden Typ von Anwendungsdienst, einschließlich Systemdienste.

Der Befehl „infacmd isp DisableService“ verwendet die folgende Syntax:

```
DisableService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Mode|-mo> disable_mode
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp DisableService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_se conds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, den Sie deaktivieren möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-Mode -mo	disable_mode	Erforderlich. Definiert, wie der Dienst deaktiviert wird: <ul style="list-style-type: none"> <li>- Abschließen. Deaktiviert den Dienst, nachdem alle Dienstprozesse gestoppt sind.</li> <li>- Stoppen. Stoppt, falls der Dienst ein PowerCenter-Integrationsdienst ist, alle ausgeführten Arbeitsabläufe und deaktiviert dann den PowerCenter-Integrationsdienst. Handelt es sich bei dem Dienst um einen Analyst-Dienst, werden alle Jobs angehalten und der Dienst wird anschließend deaktiviert.</li> <li>- Abbrechen. Stoppt alle Prozesse sofort und deaktiviert dann den Dienst.</li> </ul>

**Hinweis:** Bei Angabe von „Stopp“ als Deaktivierungsmodus für einen Listenerdienst wartet der Befehl bis zu 30 Sekunden, bis die untergeordneten Listener-Aufgaben abgeschlossen werden. Danach werden der Dienst und der Listenerdienst-Prozess heruntergefahren.

## DisableServiceProcess

Deaktiviert den Dienstprozess auf einem angegebenen Knoten.

Sie können einen Dienstprozess auf einem angegebenen Knoten deaktivieren, wenn der Knoten verwaltet werden muss.

Der Befehl „infacmd isp DisableServiceProcess“ verwendet die folgende Syntax:

```
DisableServiceProcess
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-NodeName|-nn> node_name
<-Mode|-mo> disable_mode
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp DisableServiceProcess“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des mit dem Prozess verbundenen Diensts, den Sie deaktivieren möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienstprozess ausgeführt wird.
-Mode -mo	disable_mode	Erforderlich. Definiert, wie der Dienstprozess deaktiviert wird: <ul style="list-style-type: none"> <li>- Vollständig. Ermöglicht, dass der Dienstprozess vor der Deaktivierung die aktuellen Aufgaben abschließt.</li> <li>- Stoppen. Handelt es sich bei dem Prozess um einen Integrationsdienst-Prozess, werden alle laufenden Arbeitsabläufe gestoppt und der Integrationsdienst-Prozess wird deaktiviert.</li> <li>- Abbrechen. Deaktiviert den Dienstprozess, bevor die aktuellen Aufgaben abgeschlossen werden.</li> </ul>

## DisableUser

Deaktiviert ein Benutzerkonto in der Domäne. Wenn ein Benutzer nicht vorübergehend auf die Domäne zugreifen soll, können Sie das Benutzerkonto deaktivieren.

Wenn Sie ein Benutzerkonto deaktivieren, kann der Benutzer sich nicht an den PowerCenter Anwendungen anmelden.

Der Befehl „infacmd isp DisableUser“ verwendet die folgende Syntax:

```
DisableUser
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_Name
[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
```



In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp DisableUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
ExistingUserName -eu	existing_user_name	Erforderlich. Benutzerkonto, das Sie deaktivieren möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der zu deaktivierende Benutzer gehört. Standardwert ist „Native“.

## EditUser

Bearbeitet die allgemeinen Eigenschaften für ein Benutzerkonto in der nativen Sicherheitsdomäne.

Sie können die Eigenschaften von Benutzerkonten in den LDAP-Sicherheitsdomänen nicht ändern.

Sie können den Anmeldenamen eines nativen Benutzers nicht ändern.

Der Befehl „infacmd isp EditUser“ verwendet die folgende Syntax:

```

EditUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_Name

[<-ExistingUserFullName|-ef> Existing_user_full_name]

[<-ExistingUserDescription|-ds> Existing_user_description]

[<-ExistingUserEmailAddress|-em> Existing_user_email_address]

[<-ExistingUserPhoneNumber|-pn> Existing_user_phone_number]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp EditUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_name	Erforderlich. Benutzerkonto, das Sie bearbeiten möchten.
-ExistingUserFullName -sf	existing_user_full_name	Optional. Geänderter vollständiger Name für das Benutzerkonto. Um einen Namen einzugeben, der Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen. Der vollständige Name darf folgende Sonderzeichen nicht enthalten: < > "
-ExistingUserDescription -ds	existing_user_description	Optional. Geänderte Beschreibung für das Benutzerkonto. Um eine Beschreibung einzugeben, die Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen. Die Beschreibung darf die folgenden Sonderzeichen nicht enthalten: < > "
-ExistingUserEmailAddress -em	existing_user_email_address	Optional. Geänderte E-Mail-Adresse für den Benutzer. Um eine Adresse einzugeben, die Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen. Die E-Mail-Adresse darf keines der folgenden Sonderzeichen enthalten: < > "
-ExistingUserPhoneNumber -pn	existing_user_phone_number	Optional. Geänderte Telefonnummer für den Benutzer. Um eine Telefonnummer einzugeben, die Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen. Die Telefonnummer darf die folgenden Sonderzeichen nicht enthalten: < > "

# EnableNodeResource

Aktiviert eine Informatica-Ressource. Informatica-Ressourcen beinhalten Datei- oder Verzeichnisressourcen, benutzerspezifische Ressourcen und Verbindungsressourcen. Wenn Sie eine Ressource auf einem Knoten aktivieren, kann der Load Balancer Aufgaben verteilen, die die Ressource für diesen Knoten benötigen.

Wenn ein PowerCenter-Integrationsdienst in einem Gitter ausgeführt wird, kann der Load Balancer Ressourcen verwenden, um Sitzungs-, Befehls- und vordefinierte Event-Wait-Aufgaben zu verteilen. Wenn der PowerCenter-Integrationsdienst für die Überprüfung von Ressourcen konfiguriert ist, verteilt der Load Balancer Aufgaben an Knoten, auf denen Ressourcen hinzugefügt und aktiviert werden.

Der Befehl „infacmd isp EnableNodeResource“ verwendet die folgende Syntax:

```
EnableNodeResource

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

[<-ResourceCategory|-rc> resource_category ("PCIS", "DIS")]

<-ResourceType|-rt> resource_type ("Custom", "File Directory", "Connection")

<-ResourceName|-rn> resource_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp EnableNodeResource“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem die Ressource definiert ist.
-ResourceCategory -rc	resource_category	Optional. Kategorie der Ressource. Gültige Kategorien umfassen: - PCIS. Ressource für den PowerCenter-Integrationsdienst. - DIS. Für zukünftige Verwendung reserviert. Standardwert ist PCIS.
-ResourceType -rt	resource_type	Erforderlich. Typ der Ressource. Gültige Typen umfassen: - Benutzerdefiniert - Dateiverzeichnis - Verbindung
-ResourceName -rn	resource_name	Erforderlich. Vollständiger Name der Ressource.  Um die Namen aller für einen Knoten verfügbaren Ressourcen aufzulisten, führen Sie den ListNodeResources-Befehl aus.

# EnableService

Aktiviert den Anwendungsdienst, der dem Dienstenamen entspricht.

Aktiviert jeden Typ von Anwendungsdienst, einschließlich Systemdienste. Sie können auch den Informatica Administrator aktivieren.

Der Befehl „infacmd isp EnableService“ verwendet die folgende Syntax:

```
EnableService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp EnableService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	<p>Erforderlich. Name des Diensts, den Sie aktivieren möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.</p> <p>Geben Sie zum Starten des Administrator Tools _adminconsole ein.</p>

## EnableServiceProcess

Aktiviert den Dienstprozess auf einem angegebenen Knoten.

Der Befehl „infacmd isp EnableServiceProcess“ verwendet die folgende Syntax:

```
EnableServiceProcess

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name
```



<-nodeName|-nn> node\_name

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp EnableServiceProcess“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port .. .	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_se conds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des mit dem Prozess verbundenen Diensts, den Sie aktivieren möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem Sie einen Dienstprozess aktivieren möchten.

## EnableUser

Aktiviert ein Benutzerkonto in der Domäne.

Der Befehl „infacmd isp EnableUser“ verwendet die folgende Syntax:

```
EnableUser
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_Name
[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp EnableUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
ExistingUserName -eu	existing_user_name	Erforderlich. Benutzerkonto, das Sie aktivieren möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der zu aktivierende Benutzer gehört. Standardwert ist „Native“.

## ExportDomainObjects

Exportiert native Benutzer, native Gruppen, Rollen, Verbindungen und Cluster-Konfigurationen aus der Informatica-Domäne in eine XML-Datei.

Wenn Sie nicht alle Objekte in der Domäne exportieren möchten, verwenden Sie eine infacmd-Exportsteuerdatei zum Filtern der Objekte, die Sie exportieren möchten.

Verwenden Sie die Befehle „ExportDomainObjects“ und „ImportDomainObjects“, um Objekte zwischen zwei unterschiedlichen Domänen derselben Version zu migrieren. Verwenden Sie zum Exportieren nativer Benutzer und Gruppen aus Domänen unterschiedlicher Versionen den infacmd isp ExportUsersAndGroups-Befehl.

Beim Exportieren einer Gruppe werden alle Untergruppen und Benutzer in der Gruppe exportiert.

Sie können den Administrator-Benutzer, die Administratorgruppe, die Benutzer in der Administratorgruppe, die Gruppe „Jeder“ oder die LDAP-Benutzer oder -Gruppen nicht exportieren. Um LDAP-Benutzer und -Gruppen in einer Informatica-Domäne zu replizieren, exportieren Sie die LDAP-Benutzer und -Gruppen direkt aus dem LDAP-Verzeichnisdienst.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, erhöhen Sie den verfügbaren Speicher für „infacmd“. Um den Systemspeicher zu erhöhen, legen Sie den Wert „-Xmx“ in der Umgebungsvariable ICMD\_JAVA\_OPTS fest.

Der Befehl „infacmd isp ExportDomainObjects“ verwendet die folgende Syntax:

```
ExportDomainObjects
```

```

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExportFile|-fp> export_file_name

[<-ExportControlFile|-cp> export_control_file_name]

[<-RetainPassword|-rp> retain_password]

[<-Force|-f>]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ExportDomainObjects“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p> <p>Wenn Sie für ein natives Benutzerkonto die Passwortkomplexität aktivieren, beachten Sie beim Erstellen oder Ändern eines Passworts Folgendes:</p> <ul style="list-style-type: none"> <li>- Das Passwort muss aus mindestens acht Zeichen bestehen.</li> <li>- Es muss mindestens einen Buchstaben, eine Zahl und ein nicht alphanumerisches Zeichen enthalten, z. B.:</li> </ul> <pre>! \ " # \$ % &amp; ' ( ) * + , - . / : ; &lt; = &gt; ? @ [ ] ^ _ ` {   } ~</pre> <p>Manche Sonderzeichen in Passwörtern können von der Shell anders interpretiert werden. Beispielsweise wird <code>\$</code> als Variable interpretiert. Setzen Sie in diesem Fall ein Escape-Zeichen vor das betreffende Sonderzeichen.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port .. .	<p>Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.</p>
-ResilienceTimeout -re	timeout_period_in_se conds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.</p>

Option	Argument	Beschreibung
-ExportFile -fp	export_file_name	Erforderlich. Pfad und Dateiname der Exportdatei. Wenn Sie den Dateipfad nicht angeben, erstellt infacmd die Datei in dem Verzeichnis, in dem infacmd ausgeführt wird.
-ExportControlFile -cp	export_control_file	Optional. Name und Pfad der Exportsteuerdatei, die die exportierten Objekte filtert.
-RetainPassword -rp	retain_password	Optional. Legen Sie die Option auf TRUE fest, um verschlüsselte Passwörter für Benutzer und Verbindungen in der exportierten Datei beizubehalten. Wird die Option auf FALSE festgelegt, werden Benutzer- und Verbindungspasswörter als leere Zeichenfolgen exportiert. Standardwert ist FALSE.
-Force -f	-	Optional. Überschreibt die Exportdatei, wenn eine Datei mit demselben Namen bereits vorhanden ist. Wenn Sie diese Option auslassen, werden Sie aufgefordert, das Überschreiben der Datei zu bestätigen.

## ExportUsersAndGroups

Exportiert native Benutzer und Gruppen in eine XML-Datei.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, erhöhen Sie den verfügbaren Speicher für „infacmd“. Um den Systemspeicher zu erhöhen, legen Sie den Wert „-Xmx“ in der Umgebungsvariable ICMD\_JAVA\_OPTS fest.

Der Befehl „infacmd isp ExportUsersAndGroups“ verwendet die folgende Syntax:

```
ExportUsersAndGroups
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExportFile|-ef> export_file_name
[<-Force|-f>]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ExportUsersAndGroups“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.  Wenn Sie für ein natives Benutzerkonto die Passwortkomplexität aktivieren, beachten Sie beim Erstellen oder Ändern eines Passworts Folgendes: <ul style="list-style-type: none"> <li>- Das Passwort muss aus mindestens acht Zeichen bestehen.</li> <li>- Es muss mindestens einen Buchstaben, eine Zahl und ein nicht alphanumerisches Zeichen enthalten, z. B.:  ! \ " # \$ % &amp; ' ( ) * + , - . / : ; &lt; = &gt; ?  @ [ ] ^ _ ` {   } ~</li> </ul> Manche Sonderzeichen in Passwörtern können von der Shell anders interpretiert werden. Beispielsweise wird \$ als Variable interpretiert. Setzen Sie in diesem Fall ein Escape-Zeichen vor das betreffende Sonderzeichen.



Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExportFile -ef	export_file_name	<p>Erforderlich. Name und Dateipfad, in den die Exportdatei geschrieben werden soll.</p> <p>Wenn Sie den Dateipfad nicht angeben, erstellt infacmd die Backup-Datei in dem Verzeichnis, in dem infacmd ausgeführt wird.</p>
-Force -f	-	Optional. Überschreibt die Exportdatei, wenn eine Datei mit demselben Namen bereits vorhanden ist. Wenn Sie diese Option auslassen, werden Sie aufgefordert, das Löschen der Datei zu bestätigen.

## VERWANDTE THEMEN:

- [“ImportUsersAndGroups” auf Seite 600](#)

# GetFolderInfo

Ruft Ordnerinformationen ab. Ordnerinformationen enthalten den Pfad, den Namen und die Beschreibung des Ordners.

Um den infacmd isp GetFolderInfo-Befehl auszuführen, müssen Sie über Berechtigungen für den Ordner verfügen.

Der Befehl „infacmd isp GetFolderInfo“ verwendet die folgende Syntax:

```
GetFolderInfo

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-FolderPath|-fp> full_folder_path
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetFolderInfo“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-FolderPath -fp	full_folder_path	Erforderlich. Vollständiger Pfad (ohne Domänenname) des Ordners. Folgendes Format ist obligatorisch:  <i>/parent_folder/child_folder</i>

## GetLastError

Ruft die neuesten Fehlermeldungen für einen Anwendungsdienst ab, der auf einem Knoten ausgeführt wird.

Die Fehlermeldungen sind Protokollereignisse, die eine Schweregradstufe von *error* oder *fatal* haben. Dieser Befehl gibt keine Fehler zurück, die vor dem letzten Start von Informatica-Diensten aufgetreten sind.

Sie können Fehlermeldungen in eine Datei speichern oder auf dem Bildschirm anzeigen.

Der Befehl „infacmd isp GetLastError“ verwendet die folgende Syntax:

```
GetLastError

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

[<-Format|-fm> format_TEXT_XML]

[<-MaxEvents|-me> maximum_number_of_error_events]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetLastError“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Optional. Name des Diensts, für den Sie Fehlermeldungen abrufen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienst ausgeführt wird.
-Format -fm	format	<p>Optional. Format für Fehlermeldungen. Gültige Typen umfassen:</p> <ul style="list-style-type: none"> <li>- Text</li> <li>- XML</li> </ul> <p>Wenn Sie kein Format angeben, zeigt infacmd die Nachrichten im Textformat mit einer Zeilenlänge von 80 Zeichen an.</p>
-MaxEvents -me	maximum_number_of_error_events	Optional. Maximale Anzahl abzurufender Fehlermeldungen. Der Standardwert ist 1. Der Höchstwert lautet „20“.

# GetLog

Ruft Log-Ereignisse ab. Sie können Protokollereignisse für eine Domäne oder einen Dienst erhalten. Sie können Log-Ereignisse in eine Datei schreiben oder auf dem Bildschirm anzeigen.

Um Protokollereignisse für eine Domäne abzurufen, müssen Sie über Berechtigungen für die Domäne verfügen. Um Protokollereignisse für einen Dienst abzurufen, müssen Sie über Berechtigungen für den Dienst verfügen.

Der Befehl „infacmd isp GetLog“ verwendet die folgende Syntax:

```
GetLog

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-StartDate|-sd> start_date_time]

[<-EndDate|-ed> end_date_time]

[<-ReverseOrder|-ro>]

[<-Format|-fm> format_TEXT_XML_BIN]

[<-OutputFile|-lo> output_file_name]

[<-ServiceType|-st> service_type AS|BW|CMS|DIS|ES|IS|MM|MRS|RMS|RS|SCH|SEARCH|TDM|TDW|WS|
DOMAIN]

[<-ServiceName|-sn> service_name]

[<-Severity|-svt> FATAL_ERROR_WARNING_INFO_TRACE_DEBUG]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetLog“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-StartDate -sd	start_date_time	<p>Optional. Gibt die Protokollereignisse beginnend mit dem aktuellen Datum und der aktuellen Uhrzeit zurück. Geben Sie Datum und Uhrzeit in einem der folgenden Formate ein:</p> <ul style="list-style-type: none"> <li>- MM/dd/yyyy_hh:mm:ssa_Z</li> <li>- MM/dd/yyyy_hh:mm:ssa_Z</li> <li>- MM/dd/yyyy_hh:mm:ssa</li> <li>- MM/dd/yyyy_hh:mm:ssa</li> <li>- jjjj-MM-tt_HH:mm:ss_Z</li> <li>- jjjj-MM-tt_HH:mm:ss_Z</li> <li>- jjjj-MM-tt_HH:mm:ss</li> <li>- jjjj-MM-tt_HH:mm:ss</li> <li>- MM/dd/yyyy hh:mm:ssa Z</li> <li>- MM/dd/yyyy hh:mm:ssa Z</li> <li>- MM/dd/yyyy hh:mm:ssa</li> <li>- MM/dd/yyyy hh:mm:ssa</li> <li>- jjjj-MM-tt HH:mm:ss_Z</li> <li>- jjjj-MM-tt HH:mm:ss_Z</li> <li>- jjjj-MM-tt HH:mm:ss</li> <li>- yyyy-MM-dd HH:mm</li> <li>- MM/dd/yyyy</li> <li>- jjjj-MM-tt</li> </ul> <p>Dabei ist „a“ ein am-/pm-Marker („a“ für a.m. und „p“ für p.m.) und „Z“ ein Zeitzone-Marker (z. B. „-0800“ oder „GMT“).</p>
-EndDate -ed	end_date_time	<p>Optional. Gibt die Protokollereignisse zurück, die bis zu diesem Datum und dieser Uhrzeit enden. Geben Sie Datum und Uhrzeit im selben Format wie die StartDate-Option ein.</p> <p>Wenn Sie ein Enddatum eingeben, das vor dem Startdatum liegt, gibt GetLog keine Protokollereignisse zurück.</p>
-ReverseOrder -ro	-	Optional. Ruft Protokollereignisse entsprechend dem aktuellen Zeitstempel ab.
-Format -fm	format	<p>Optional. Format für Protokollereignisse. Gültige Typen umfassen:</p> <ul style="list-style-type: none"> <li>- Text</li> <li>- XML</li> <li>- Bin (binär)</li> </ul> <p>Wenn Sie „Binär“ auswählen, müssen Sie einen Dateinamen mithilfe der OutputFile-Option angeben.</p> <p>Wenn Sie kein Format angeben, verwendet infacmd Textformat mit einer Zeilenlänge von 80 Zeichen.</p>



Option	Argument	Beschreibung
-OutputFile -lo	output_file_name	Name und Dateipfad, in den die Protokolldatei geschrieben werden soll. Standardmäßig verwendet der Dienstmanager das Verzeichnis „server\infa_shared\log“ auf dem Master-Gateway-Knoten.  Lassen Sie diese Option aus, um die Protokollereignisse auf dem Bildschirm anzuzeigen.  Wenn Sie „Binär“ als Ausgabedateityp auswählen, müssen Sie einen Dateinamen mithilfe dieser Option angeben.
-ServiceType -st	service_type	Optional. Typ des Diensts, für den Sie Protokollereignisse abrufen möchten. Sie können einen Diensttyp angeben.  Lassen Sie diese Option aus, um Protokollereignisse für alle Diensttypen abzurufen.  Zu den Diensttypen gehören: <ul style="list-style-type: none"> <li>- AS. Analyst-Dienst</li> <li>- BW. SAP BW-Dienst</li> <li>- CMS. Content-Managementdienst</li> <li>- DIS. Datenintegrationsdienst</li> <li>- ES. E-Mail-Dienst</li> <li>- IS. PowerCenter-Integrationsdienst</li> <li>- MM. Metadata Manager-Dienst</li> <li>- MRS. Modellrepository-Dienst</li> <li>- RMS. Ressourcenmanager-Dienst</li> <li>- RS. PowerCenter-Repository-Dienst</li> <li>- SCH. Scheduler-Dienst</li> <li>- SEARCH. Suchdienst</li> <li>- TDM. Test Data Manager-Dienst</li> <li>- TDW. Test Data Warehouse-Dienst</li> <li>- WS. Webdienst-Hub</li> <li>- DOMAIN. Domäne</li> </ul>
-ServiceName -sn	service_name	Optional. Name des Diensts, für den Sie Protokollereignisse abrufen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-Severity -svt	severity_level	Optional. Schweregrad von Meldungen. Schweregradtypen umfassen: <ul style="list-style-type: none"> <li>- Schwerwiegend</li> <li>- Fehler</li> <li>- Warnung</li> <li>- Info</li> <li>- Trace</li> <li>- Debug</li> </ul>

## GetNodeName

Gibt den Namen eines Knotens zurück.

Ruft den Knotennamen aus der nodemeta.xml-Datei auf dem Knoten ab. Sie müssen diesen Befehl auf dem Knoten eingeben, für den Sie den Namen abrufen möchten.

Der infacmd isp GetNodeName-Befehl verwendet die folgende Syntax:

```
GetNodeName  
[<-OutputFile|-o>] output_file
```

Wenn Sie den Befehl ohne die Option -o verwenden, druckt der Befehl den Knotennamen in das Befehlsfenster. Wenn Sie die Option -o zum Angeben einer Ausgabedatei verwenden, geben Sie den Dateinamen und den Pfad an. Beispiel:

```
isp\bin\infacmd.bat getNodeName -o c:\node_name.txt
```

Der Befehl erstellt unter dem von Ihnen angegebenen Pfad eine Datei mit der Bezeichnung „node\_name.txt“. Er druckt den Knotennamen in die Datei. Falls die Datei vorhanden ist, überschreibt der Befehl sie.

## GetPasswordComplexityConfig

Gibt die Konfiguration der Passwortkomplexität für die Domänenbenutzer zurück.

Der Befehl in „facmd GetPasswordComplexityConfig“ verwendet die folgende Syntax:

```
GetPasswordComplexityConfig  
<-DomainName|-dn> domain_name  
<-UserName|-un> user_name  
<-Password|-pd> password  
[<-SecurityDomain|-sdn> security_domain]  
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd GetPasswordComplexityConfig“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domännennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domännennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Geben Sie die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne an.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariablen INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang. Standardwert ist 180 Sekunden.

## getDomainSamlConfig

Gibt den Status SAML-Authentifizierungsstatus (Secure Assertion Markup Language) für eine Informatica-Domäne zurück. Wenn die SAML-Authentifizierung aktiviert ist, gibt der Befehl auch die Identitätsanbieter-URL und den zulässigen zeitlichen Unterschied zwischen der Systemuhr des Identitätsanbieter-Hosts und der Systemuhr des Master-Gateway-Knotens zurück.

Führen Sie den Befehl auf einem beliebigen Gateway-Knoten innerhalb der Informatica-Domäne aus. Sie können diesen Befehl nur mit der Administratorrolle ausführen.

Der Befehl „infacmd isp getDomainSamlConfig“ verwendet die folgende Syntax:

```
getDomainSamlConfig
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
[<-SecurityDomain|-sdn> security_domain]
<-Password|-pd> password
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp getDomainSamlConfig“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.inf“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

# GetServiceOption

Ruft den Wert einer Diensteseigenschaft für einen PowerCenter-Integrationsdienst, PowerCenter-Repository-Dienst, SAP BW-Dienst oder Webdienst-Hub ab. Führen Sie für Datenintegrationsdienst- oder Analyst-Dienst-Optionen „infacmd dis“ oder „infacmd“ als ListServiceOptions aus.

Sie können beispielsweise den Repository-Datenbanktyp abrufen.

Der Befehl „infacmd isp GetServiceOption“ verwendet die folgende Syntax:

```
GetServiceOption

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-OptionName|-op> option_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetServiceOption“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port .. .	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, für den Sie einen Wert abrufen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-OptionName -op	option_name	<p>Erforderlich. Name der Option, für die Sie einen Wert abrufen möchten. Die angegebenen Optionen richten sich nach dem Diensttyp:</p> <ul style="list-style-type: none"> <li>- Weitere Informationen zu den Optionen des Integrationsdiensts finden Sie unter <a href="#">"Integrationsdienst-Optionen" auf Seite 506</a>.</li> <li>- Für einen SAP BW-Dienst geben Sie „BWSystemConXString“ (den R-Typ für SAP-Ziel) oder „RetryPeriod“ (den Wiederholungszeitraum in Sekunden) ein.</li> <li>- Weitere Informationen zu den Optionen des Webdienst-Hubs finden Sie unter <a href="#">"Web Services Hub-Optionen" auf Seite 538</a>.</li> </ul>

## GetServiceProcessOption

Ruft den Wert für eine Eigenschaft auf einem PowerCenter-Integrationsdienst-Prozess ab, der auf einem Knoten ausgeführt wird.

Der Befehl „infacmd isp GetServiceProcessOption“ verwendet die folgende Syntax:

```
GetServiceProcessOption
<-DomainName|-dn> domain_name
```

```

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

<-OptionName|-op> option_name

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetServiceProcessOption“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port .. .	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_se conds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, für den Sie einen Wert abrufen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienstprozess ausgeführt wird.
-OptionName -op	option_name	Erforderlich. Name der Option, für die Sie einen Wert abrufen möchten.

## VERWANDTE THEMEN:

- [“Integration Service-Prozessoptionen” auf Seite 511](#)

# GetServiceProcessStatus

Ruft den Status eines Anwendungsdienstprozesses auf einem Knoten ab. Ein Dienstprozess kann aktiviert oder deaktiviert werden.

Der Befehl „infacmd isp GetServiceProcessStatus“ verwendet die folgende Syntax:

```
GetServiceProcessStatus
<-DomainName|-dn> domain_name
```



```

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetServiceProcessStatus“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port .. .	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_se conds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, der den Prozess ausführt, für den Sie den Status abrufen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienstprozess ausgeführt wird.

## GetServiceStatus

Ruft den Status eines Anwendungsdiensts ab.

Sie können den Status eines Dienst abrufen, z. B. des Repository-Diensts, des Datenintegrationsdiensts, des Analyst-Diensts, des Integrationsdiensts, des Webdienst-Hub oder des SAP BW-Diensts. Ein Dienst kann aktiviert oder deaktiviert werden.

Der Befehl „infacmd isp GetServiceStatus“ verwendet die folgende Syntax:

```
GetServiceStatus
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetServiceStatus“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, für den Sie den Status abrufen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

## GetSessionLog

Ruft Log-Ereignisse für eine Sitzung ab, die zuletzt ausgeführt wurde. Der PowerCenter-Repository-Dienst muss bei Ausführung dieses Befehls ausgeführt werden.

Der Befehl „infacmd isp GetSessionLog“ verwendet die folgende Syntax:

```
GetSessionLog
<-DomainName|-dn> domain_name
[<-UserName|-un> user_name]
[<-Password|-pd> password]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-Format|-fm> format_TEXT_XML_BIN]
[<-OutputFile|-lo> output_file_name]
<-IntegrationService|-is> integration_service_name
<-RepositoryService|-rs> repository_service_name
[<-RepositoryDomain|-rd> domain_of_repository]
<-RepositoryUser|-ru> repository_user]
<-RepositoryPassword|-rp> repository_password]
[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]
<-FolderName|-fn> repository_folder_name
<-Workflow|-wf> workflow_name
[<-RunInstance|-in> run_instance_name] | <-RunId|-id> workflow_run_id]
<-Session|-ss> session_name
```

**Hinweis:** Wenn Sie die Optionen -un, -pd und -sdn nicht festlegen, verwendet der infacmd isp GetSessionLog-Befehl die entsprechenden Werte aus den Optionen -ru, -rp und -rsdn options.

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetSessionLog“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-Format -fm	format	Optional. Format für das Sitzungsprotokoll. Gültige Typen umfassen: <ul style="list-style-type: none"> <li>- Text</li> <li>- XML</li> <li>- Bin (binär)</li> </ul> Wenn Sie „Binär“ auswählen, müssen Sie einen Dateinamen mithilfe der OutputFile-Option angeben. Wenn Sie kein Format angeben, verwendet <i>infacmd</i> Textformat mit einer Zeilenlänge von 80 Zeichen.
-OutputFile -lo	output_file_name	Name und Dateipfad für die Sitzungsprotokolldatei. Standardmäßig verwendet der Dienstmanager das Verzeichnis „server\infa_shared\log“ auf dem Master-Gateway-Knoten. Lassen Sie diese Option aus, um die Protokollereignisse auf dem Bildschirm anzuzeigen. Wenn Sie „Binär“ als Ausgabedateityp auswählen, müssen Sie einen Dateinamen mithilfe dieser Option angeben.
-IntegrationService -is	integration_service_name	Erforderlich. Name des Integrationsdiensts, der die Sitzung ausführt. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryService -rs	repository_service_name	Erforderlich. Name des Repository-Diensts, der die Sitzung enthält. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryDomain -rd	domain_of_repository	Erforderlich, wenn das Repository sich in einer anderen als der lokalen Domäne befindet. Domäne des Repository-Diensts. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryUser -ru	repository_user	Erforderlich für native und LDAP-Authentifizierung. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zum Repository. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

Option	Argument	Beschreibung
-RepositoryPassword -rp	repository_password	Erforderlich für native und LDAP-Authentifizierung. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Benutzerpasswort. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -rp festgelegte Passwort Vorrang.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Erforderlich für LDAP- oder Kerberos-Authentifizierung. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der PowerCenter-Repository-Benutzer gehört.  Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn Sie diese Option nicht angeben, setzt der Befehl die Sicherheitsdomäne des Repository-Benutzers auf nativ.
-FolderName -fn	repository_folder_name	Erforderlich. Name des Ordners, der die Sitzung enthält. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-Workflow -wf	workflow_name	Erforderlich. Name des Arbeitsablaufs, der die Sitzung enthält. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RunInstance -in	run_instance_name	Name der Arbeitsablaufausführungsinstanz, die die Sitzung enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. Verwenden Sie die Option -in oder die Option -id, jedoch nicht beide.
-RunId -id	workflow_run_id	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus, die die Sitzung enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. Verwenden Sie die Option -in oder die Option -id, jedoch nicht beide. <b>Hinweis:</b> Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-Session -ss	session_name	Erforderlich. Sitzungsname. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

## GetSystemLogDirectory

Gibt den Pfad des Systemprotokollverzeichnis zurück.

Geben Sie diesen Befehl in der Domäne ein, deren Verzeichnispfad für Systemprotokolle abgerufen werden soll.

Der infacmd isp GetSystemLogDirectory-Befehl verwendet die folgende Syntax:

```
GetSystemLogDirectory  
[<-OutputFile|-o> output_file]
```

Wenn Sie den Befehl ohne die Option -o verwenden, zeigt der Befehl den Verzeichnispfad im Befehlsfenster an. Wenn Sie die Option -o zum Angeben einer Ausgabedatei verwenden, stellen Sie den Dateinamen und den Pfad für die Ausgabedatei bereit. Beispiel:

```
isp\bin\infacmd.bat getSystemLogDirectory -o c:\sys_log_dir.txt
```

Der Befehl erstellt die Datei „sys\_log\_dir.txt“ im angegebenen Pfad und zeigt den Pfad des Systemprotokollverzeichnisses in der Datei an. Wenn die Datei vorhanden ist, wird sie vom Befehl überschrieben.

## getUserActivityLog

Ruft Benutzeraktivitätsprotokolle für einen einzelnen oder mehrere Benutzer ab. Sie können Benutzeraktivitätsprotokolle in eine Datei schreiben oder in der Konsole anzeigen.

Die Benutzeraktivitätsprotokolle enthalten erfolgreiche und fehlgeschlagene Anmeldeversuche von Informatica-Clients. Wenn der Client benutzerdefinierte Eigenschaften einschließt, die bei Anmeldeanfragen von den Clients festgelegt werden, enthält die Daten die betreffenden Eigenschaften.

**Hinweis:** In einer Domäne, die für die Verwendung der Kerberos-Authentifizierung konfiguriert ist, werden Anmeldeversuche von Benutzern nicht in den Benutzeraktivitätsprotokollen aufgezeichnet.

Der Befehl „infacmd isp getUserActivityLog“ verwendet die folgende Syntax:

```
getUserActivityLog  
<-DomainName|-dn> domain_name  
<-UserName|-un> user_name  
<-Password|-pd> password  
[<-SecurityDomain|-sdn> security_domain]  
[<-Gateway|-hp> gateway_host1:port]  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]  
[<-Users|-usrs> user1:[securitydomain] user2:[securitydomain]...  
[<-StartDate|-sd> start_date]  
[<-EndDate|-ed> end_date]  
[<-ActivityCode|-ac> activity_code]  
[<-ActivityText|-atxt> activity_text]  
[<-ReverseOrder|-ro> true]  
[<-OutputFile|-lo> output_file_name]  
[<-Format|-fm> output_format_BIN_TEXT_XML]
```



In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp getUserActivityLog“ beschrieben:

Option	Argument	Beschreibung
- DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
- SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
- ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-Users -usrs	user1:[securitydomain] user2:[securitydomain] ...	<p>Optional. Die Liste der Benutzer, für die Sie Protokollereignisse erhalten möchten. Trennen Sie mehrere Benutzer mit einem Leerzeichen. Verwenden Sie das Platzhaltersymbol (*), um Protokolle für mehrere Benutzer in einer einzelnen Sicherheitsdomäne oder in allen Sicherheitsdomänen anzuzeigen. Beispiel: Die folgenden Zeichenfolgen sind gültige Werte für diese Option:</p> <pre> user:Native "user:*" "user*" "*_users_*" "*:Native" </pre> <p>Wenn Sie das Platzhaltersymbol verwenden, setzen Sie das Argument in Anführungszeichen.</p> <p>Wenn Sie keinen Benutzer eingeben, ruft der Befehl die Protokollereignisse für alle Benutzer ab.</p>
-StartDate -sd	start_date	<p>Optional. Gibt die Protokollereignisse beginnend mit dem Datum und der Uhrzeit zurück, die Sie angegeben haben.</p> <p>Geben Sie das Datum und die Uhrzeit in einem der folgenden Formate ein:</p> <ul style="list-style-type: none"> <li>- MM/tt/jjjj</li> <li>- MM/tt/jjjj HH:mm:ss</li> <li>- jjjj-MM-tt</li> <li>- jjjj-MM-tt HH:mm:ss</li> </ul>
-EndDate -ed	end_date	<p>Optional. Gibt die Protokollereignisse zurück, die bis zu diesem Datum und dieser Uhrzeit enden. Geben Sie Datum und Uhrzeit im selben Format wie die Option „Startdatum“ ein.</p> <p>Wenn Sie ein Enddatum eingeben, das vor dem Startdatum liegt, gibt der Befehl keine Protokollereignisse zurück.</p>
-ActivityCode -ac	activity_code	<p>Optional. Gibt Protokollereignisse auf Basis des Aktivitätscodes zurück.</p> <p>Verwenden Sie das Platzhaltersymbol (*), um Protokollereignisse für mehrere Aktivitätscodes abzurufen. Gültige Aktivitätscodes:</p> <ul style="list-style-type: none"> <li>- CCM_10437. Gibt an, dass eine Aktivität erfolgreich war.</li> <li>- CCM_10438. Gibt an, dass eine Aktivität fehlgeschlagen ist.</li> <li>- CCM_10778. Gibt an, dass ein Anmeldeversuch mit benutzerdefinierten Eigenschaften erfolgreich war.</li> <li>- CCM_10779. Gibt an, dass ein Anmeldeversuch mit benutzerdefinierten Eigenschaften fehlgeschlagen ist.</li> <li>- CCM_10786. Gibt an, dass ein Anmeldeversuch ohne benutzerdefinierte Eigenschaften erfolgreich war.</li> <li>- CCM_10787. Gibt an, dass ein Anmeldeversuch ohne benutzerdefinierte Eigenschaften fehlgeschlagen ist.</li> </ul>

Option	Argument	Beschreibung
-atxt	activity_text	<p>-ActivityText</p> <p>Optional. Gibt die Protokollereignisse auf Basis einer im Aktivitätstext gefundenen Zeichenfolge zurück.</p> <p>Verwenden Sie das Platzhaltersymbol (*), um Protokolle für mehrere Ereignisse abzurufen. Beispiel: Der folgende Parameter gibt alle Protokollereignisse zurück, die „Dienst wird aktiviert“ in ihrer Beschreibung enthalten:</p> <p>"*Enabling service"</p> <p>Wenn Sie das Platzhaltersymbol verwenden, setzen Sie das Argument in Anführungszeichen.</p>
-ReverseOrder -ro	Wahr	Optional. Druckt Protokollereignisse in umgekehrter chronologischer Reihenfolge. Wenn Sie diesen Parameter nicht angeben, zeigt der Befehl Protokollereignisse in chronologischer Reihenfolge an.
-OutputFile -lo	output_file_name	Optional. Name der Ausgabedatei. Wenn Sie diesen Parameter nicht angeben, zeigt der Befehl das Protokoll in der Befehlszeile an.
-Format -fm	output_format_BIN_TEXT_XML	<p>Optional. Format der Protokollausgabedatei.</p> <p>Gültige Formate umfassen:</p> <ul style="list-style-type: none"> <li>- Bin (binär)</li> <li>- Text</li> <li>- XML</li> </ul> <p>Das Standardformat lautet „Text“. Wenn Sie das Format auf „Binär“ festlegen, müssen Sie einen Dateinamen mit der -OutputFile-Option angeben.</p>

## GetWorkflowLog

Ruft Log-Ereignisse für einen Arbeitsablauf ab, der zuletzt ausgeführt wurde. Der PowerCenter-Repository-Dienst muss bei Ausführung dieses Befehls ausgeführt werden.

Der Befehl „infacmd isp GetWorkflowLog“ verwendet die folgende Syntax:

```
GetWorkflowLog
<-DomainName|-dn> domain_name
[<-UserName|-un> user_name]
[<-Password|-pd> password]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-Format|-fm> format_TEXT_XML_BIN]
[<-OutputFile|-lo> output_file_name]
<-IntegrationService|-is> integration_service_name
```

```

<-RepositoryService|-rs> repository_service_name

[<-RepositoryDomain|-rd> domain_of_repository]

<-RepositoryUser|-ru> repository_user

<-RepositoryPassword|-rp> repository_password

[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]

<-FolderName|-fn> repository_folder_name

<-Workflow|-wf> workflow_name

[<-RunInstance|-in> run_instance_name] | [<-RunId|-id> workflow_run_id]

```

**Hinweis:** Wenn Sie die Optionen „-un“, „-pd“ und „-sdn“ nicht festlegen, verwendet der Befehl „infacmd isp GetWorkflowLog“ die entsprechenden Werte aus den Optionen „-ru“, „-rp“ und „-rsdn“.

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetWorkflowLog“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-Format -fm	format	<p>Optional. Format für das Sitzungsprotokoll. Gültige Typen umfassen:</p> <ul style="list-style-type: none"> <li>- Text</li> <li>- XML</li> <li>- Bin (binär)</li> </ul> <p>Wenn Sie „Binär“ auswählen, müssen Sie einen Dateinamen mithilfe der OutputFile-Option angeben.</p> <p>Wenn Sie kein Format angeben, verwendet <i>infacmd</i> Textformat mit einer Zeilenlänge von 80 Zeichen.</p>
-OutputFile -lo	output_file_name	Name und Dateipfad für die Arbeitsablaufprotokolldatei. Standardmäßig verwendet der Dienstmanager das Verzeichnis „server\infa_shared\log“ auf dem Master-Gateway-Knoten. Lassen Sie diese Option aus, um die Protokollereignisse auf dem Bildschirm anzuzeigen. Wenn Sie „Binär“ als Ausgabedateityp auswählen, müssen Sie einen Dateinamen mithilfe dieser Option angeben.
-IntegrationService -is	integration_service_name	Erforderlich. Name des Integrationsdiensts, der den Arbeitsablauf ausführt. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryService -rs	repository_service_name	Erforderlich. Name des Repository-Diensts, der den Arbeitsablauf enthält. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

Option	Argument	Beschreibung
-RepositoryDomain -rd	domain_of_repository	Erforderlich, wenn das Repository sich in einer anderen als der lokalen Domäne befindet. Domäne des Repository-Diensts. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryUser -ru	user	Erforderlich für native und LDAP-Authentifizierung. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zum Repository. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryPassword -rp	Passwort	Erforderlich für native und LDAP-Authentifizierung. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Benutzerpasswort. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -rp festgelegte Passwort Vorrang.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Erforderlich für LDAP- oder Kerberos-Authentifizierung. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der PowerCenter-Repository-Benutzer gehört.  Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn Sie diese Option nicht angeben, setzt der Befehl die Sicherheitsdomäne des Repository-Benutzers auf nativ.
-FolderName -fn	repository_folder_name	Erforderlich. Name des Ordners, der den Arbeitsablauf enthält. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-Workflow -wf	workflow_name	Erforderlich. Name des Arbeitsablaufs. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RunInstance -in	run_instance_name	Name der Arbeitsablaufausführungsinstanz Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. Verwenden Sie die Option -in oder die Option -id, jedoch nicht beide.
-RunId -id	workflow_run_id	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. Verwenden Sie die Option -in oder die Option -id, jedoch nicht beide. <b>Hinweis:</b> Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.

# Hilfe

Zeigt die Optionen und Argumente für einen infacmd-Befehl an.

Wenn Sie den Befehlsnamen auslassen, listet infacmd alle Befehle auf.

Der infacmd Help-Befehl verwendet die folgende Syntax:

```
Help <-plugin_ID> [command]
```

Wenn Sie beispielsweise `infacmd isp Help GetServiceStatus` eingeben, gibt infacmd die folgenden Optionen und Argumente für den infacmd isp GetServiceStatus-Befehl zurück:

```
GetServiceStatus
<-DomainName|-dn> domain_name <-UserName|-un> user_name <-Password|-pd> password [<-
Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds] <-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die infacmd Help-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-	plugin_ID	Optional. Beschreibt, für welches infacmd-Programm Hilfe angezeigt werden soll. Standardwert ist „isp“.
-	command	Optional. Name des Befehls. Wenn Sie den Befehlsnamen auslassen, listet infacmd alle Befehle auf.

## ImportDomainObjects

Importiert native Benutzer, native Gruppen, Rollen, Verbindungen und Cluster-Konfigurationen aus einer XML-Datei in eine Informatica-Domäne.

Wenn Sie nicht alle Objekte in der Datei importieren möchten, verwenden Sie eine infacmd-Importsteuerdatei zum Filtern der Objekte, die Sie importieren möchten.

Verwenden Sie die Befehle „ExportDomainObjects“ und „ImportDomainObjects“, um Objekte zwischen zwei unterschiedlichen Domänen derselben Version zu migrieren. Verwenden Sie zum Importieren nativer Benutzer und Gruppen aus Domänen unterschiedlicher Versionen den infacmd isp ImportUsersAndGroups-Befehl.

Beim Importieren einer Gruppe werden alle Untergruppen und Benutzer in der Gruppe importiert.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, erhöhen Sie den verfügbaren Speicher für „infacmd“. Um den Systemspeicher zu erhöhen, legen Sie den Wert „-Xmx“ in der Umgebungsvariable ICMD\_JAVA\_OPTS fest.

Der Befehl „infacmd isp ImportDomainObjects“ verwendet die folgende Syntax:

```
ImportDomainObjects
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

[<-ResilienceTimeout|-re> timeout\_period\_in\_seconds]

<-ImportFilePath|-fp> import\_file\_path

[<-ImportControlFile|-cp> import\_control\_file]

[<-ConflictResolution|-cr> resolution\_type]

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ImportDomainObjects“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>



Option	Argument	Beschreibung
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p> <p>Wenn Sie für ein natives Benutzerkonto die Passwortkomplexität aktivieren, beachten Sie beim Erstellen oder Ändern eines Passworts Folgendes:</p> <ul style="list-style-type: none"> <li>- Das Passwort muss aus mindestens acht Zeichen bestehen.</li> <li>- Es muss mindestens einen Buchstaben, eine Zahl und ein nicht alphanumerisches Zeichen enthalten, z. B.:  ! \ " # \$ % &amp;  ' ( ) * + ,  - . / : ; &lt; = &gt; ?  @ [ ] ^ _ ` {   }  ~</li> </ul> <p>Manche Sonderzeichen in Passwörtern können von der Shell anders interpretiert werden. Beispielsweise wird \$ als Variable interpretiert. Setzen Sie in diesem Fall ein Escape-Zeichen vor das betreffende Sonderzeichen.</p>

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“.</p> <p>Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	<p>Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.</p>

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ImportFilePath -fp	import_file_path	Erforderlich. Pfad und Dateiname der XML-Datei, aus der Sie die Objekte importieren.
-ImportControlFile -cp	import_control_file	Optional. Pfad und Dateiname der Importsteuerungsdatei, die die zu importierenden Objekte filtert.
-ConflictResolution -cr	resolution_type	<p>Optional. Konfliktlösungsstrategie. Sie können eine der folgenden Optionen angeben:</p> <ul style="list-style-type: none"> <li>- umbenennen</li> <li>- ersetzen</li> <li>- erneut verwenden</li> </ul> <p>Die Option wird ignoriert, wenn Sie eine Konfliktlösungsstrategie in der Importsteuerdatei angeben. Wenn Sie keine Konfliktlösungsstrategie definieren und ein Konflikt auftritt, schlägt der Import fehl.</p> <p><b>Hinweis:</b> Sie können die Option Umbenennen nicht mit einer Cluster-Konfiguration verwenden.</p> <p><b>Hinweis:</b> Die Passwortkomplexität ist nicht erforderlich, wenn Sie die Wiederverwendungsoption verwenden.</p>

# ImportUsersAndGroups

Importiert native Benutzer und Gruppen in die Domäne.

Führen Sie „infacmd isp ImportUsersAndGroups“ aus, um Benutzer und Gruppen aus einer XML-Datei zu importieren.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, erhöhen Sie den verfügbaren Speicher für „infacmd“. Um den Systemspeicher zu erhöhen, legen Sie den Wert „-Xmx“ in der Umgebungsvariable ICMD\_JAVA\_OPTS fest.

Der Befehl „infacmd isp ImportUsersAndGroups“ verwendet die folgende Syntax:

```
ImportUsersAndGroups
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExportFile|-ef> export_file_name
[<-ReuseDomainUsersAndGroups|-rd> If there is a conflict use the users and groups
defined in the target domain]
[<-exportedFromPowercenter|-epc> The export file containing users and groups has been
exported from an Informatica PowerCenter 8.6.1 domain]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ImportUsersAndGroups“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p> <p>Wenn Sie für ein natives Benutzerkonto die Passwortkomplexität aktivieren, beachten Sie beim Erstellen oder Ändern eines Passworts Folgendes:</p> <ul style="list-style-type: none"> <li>- Das Passwort muss aus mindestens acht Zeichen bestehen.</li> <li>- Es muss mindestens einen Buchstaben, eine Zahl und ein nicht alphanumerisches Zeichen enthalten, z. B.:</li> </ul> <pre>! \ " # \$ % &amp; ' ( ) * + , - . / : ; &lt; = &gt; ? @ [ ] ^ _ ` {   } ~</pre> <p>Manche Sonderzeichen in Passwörtern können von der Shell anders interpretiert werden. Beispielsweise wird \$ als Variable interpretiert. Setzen Sie in diesem Fall ein Escape-Zeichen vor das betreffende Sonderzeichen.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	<p>Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.</p>

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExportFile -ef	export_file_name	Erforderlich. Name und Dateipfad der Exportdatei, die Informationen über die Benutzer und Gruppen enthält.
-ReuseDomainUsersAndGroups -rd	-	Optional. Wenn ein Namenskonflikt besteht, behält infacmd die in der Zieldomäne definierten Benutzer und Gruppen bei. Der Befehl schlägt standardmäßig fehl, wenn ein Konflikt auftritt.
-exportedFromPowercenter -epc	-	Erforderlich, wenn die Exportdatei aus einer PowerCenter-Domäne der Version 8.6.1 exportiert wurde.

## VERWANDTE THEMEN:

- [“ExportUsersAndGroups” auf Seite 563](#)

# ListAlertUsers

Listet Benutzer auf, die Alarmer abonnieren.

Der Befehl „infacmd isp ListAlertUsers“ verwendet die folgende Syntax:

```
ListAlertUsers
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListAlertUsers“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

# listAllCustomLDAPTypes

Listet die Konfigurationsinformationen für alle benutzerdefinierten LDAP-Typen auf, die von der angegebenen Domäne verwendet werden.

Der Befehl „infacmd isp ListLDAPConnectivity“ verwendet die folgende Syntax:

```
listAllCustomLDAPTypes
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp listAllCustomLDAPTypes“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.



Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

## ListAllGroups

Listet alle Gruppen in der nativen Sicherheitsdomäne auf.

Der Befehl „infacmd isp ListAllGroups“ verwendet die folgende Syntax:

```
ListAllGroups
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListAllGroups“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

# listAllLDAPConnectivity

Listet die Konfigurationsinformationen für alle LDAP-Konfigurationen auf, die von der angegebenen Domäne verwendet werden.

Der Befehl „infacmd isp ListLDAPConnectivity“ verwendet die folgende Syntax:

```
listAllLDAPConnectivity
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp listAllLDAPConnectivity“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

## ListAllRoles

Listet alle Rollen in der Domäne auf.

Der Befehl „infacmd isp ListAllRoles“ verwendet die folgende Syntax:

```
ListAllRoles
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListAllRoles“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

# ListAllUsers

Listet alle Benutzerkonten in der Domäne auf.

Der Befehl „infacmd isp ListAllUsers“ verwendet die folgende Syntax:

```
ListAllUsers  
  
<-DomainName|-dn> domain_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-SecurityDomain|-sdn> security_domain]  
  
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListAllUsers“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

## ListConnectionOptions

Listet Optionen für eine Verbindung auf. Führen Sie diesen Befehl aus, um verfügbare Optionen anzuzeigen, die beim Update einer Verbindung konfiguriert werden können.

Der Befehl „infacmd isp ListConnectionOptions“ verwendet die folgende Syntax:

```
ListConnectionOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConnectionName|-cn> connection_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListConnectionOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.



Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ConnectionName -cn	connection_name_security_domain	Erforderlich. Name der Verbindung.

## ListConnectionPermissions

Listet alle Berechtigungen auf, die ein Benutzer oder eine Gruppe für die Verbindung besitzen.

Der Befehl „infacmd isp ListConnectionPermissions“ verwendet die folgende Syntax:

```
ListConnectionPermissions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<<-RecipientUserName|-run> recipient_user_name|<RecipientGroupName|-rgn>
recipient_group_name>
<-RecipientSecurityDomain|-rsd> recipient_security_domain]
<-ConnectionName|-cn> connection_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListConnectionPermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RecipientUserName -run	recipient_user_name	Erforderlich, wenn Sie den Gruppennamen des Empfängers nicht angeben. Name des Benutzers, für den Berechtigungen aufgelistet werden.
-RecipientGroupName -rgn	recipient_group_name	Erforderlich, wenn Sie den Benutzernamen des Empfängers nicht angeben. Name der Gruppe, für die Berechtigungen aufgelistet werden.
-RecipientSecurityDomain -rsd	recipient_security_domain_name	Erforderlich, wenn der Empfänger zu einer LDAP-Sicherheitsdomäne gehört. Name der Sicherheitsdomäne, zu der der Empfänger gehört. Standardwert ist „Native“.
-ConnectionName -cn	connection_name_security_domain	Erforderlich. Name der Verbindung.

## ListConnectionPermissionsByGroup

Listet alle Gruppen mit Verbindungsberechtigungen sowie den jeweiligen Verbindungstyp auf.

Der Befehl „infacmd isp ListConnectionPermissionsByGroup“ verwendet die folgende Syntax:

```
ListConnectionPermissionsByGroup
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConnectionName|-cn> connection_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListConnectionPermissionsByGroup“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ConnectionName -cn	connection_name_security_domain	Erforderlich. Name der Verbindung.

## ListConnectionPermissionsByUser

Listet alle Benutzer mit Verbindungsberechtigungen sowie den jeweiligen Verbindungstyp auf.

Der Befehl „infacmd isp ListConnectionPermissionsByUser“ verwendet die folgende Syntax:

```
ListConnectionPermissionsByUser
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConnectionName|-cn> connection_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListConnectionPermissionsByUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ConnectionName -cn	connection_name_security_domain	Erforderlich. Name der Verbindung.

## ListConnections

Listet die Verbindungsnamen nach Typ auf. Sie können eine Liste nach allen Verbindungstypen erstellen oder die Ergebnisse nach einem Verbindungstyp filtern.

Der Befehl „infacmd isp ListConnections“ verwendet die folgende Syntax:

```
ListConnections
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-ConnectionType|-ct> connection_type]
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListConnections“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ConnectionType -ct	connection_type	Optional. Sie können Ergebnisse mit der Option -ct filtern. Verwenden Sie einen beliebigen unterstützten Verbindungstyp als Wert für die Option -ct. Bei der Eingabe wird die Groß- und Kleinschreibung nicht beachtet.  Führen Sie den folgenden Befehl aus, um eine Liste der mit dieser Option zu verwendenden Verbindungstypen anzuzeigen:  <code>./infacmd.sh isp listConnections</code>  Der Befehl listet alle Verbindungstypen auf sowie die Verbindungen, die Sie in der Domäne konfiguriert haben.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.



# ListConnectionOptions

Listet Optionen für eine Verbindung auf. Führen Sie diesen Befehl aus, um verfügbare Optionen anzuzeigen, die beim Update einer Verbindung konfiguriert werden können.

Der Befehl „infacmd isp ListConnectionOptions“ verwendet die folgende Syntax:

```
ListConnectionOptions  
  
<-DomainName|-dn> domain_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-SecurityDomain|-sdn> security_domain]  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]  
  
<-ConnectionName|-cn> connection_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListConnectionOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ConnectionName -cn	connection_name_security_domain	Erforderlich. Name der Verbindung.

## listCustomLDAPType

Listet die Konfigurationsinformationen für einen benutzerdefinierten LDAP-Typ auf.

Der Befehl „infacmd isp listCustomLDAPType“ verwendet die folgende Syntax:

```
listCustomLDAPType
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-CustomLDAPTypeName|-lt> custom_LDAP_type_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp listCustomLDAPType“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-CustomLDAPTypeName -lt	Name des benutzerdefinierten LDAP-Typs	Erforderlich. Der Name des benutzerdefinierten LDAP-Typs.

## ListDefaultOSProfiles

Listet die Standardbetriebssystemprofile für den angegebenen Benutzer bzw. die angegebene Gruppe auf.

Der Befehl „infacmd isp ListDefaultOSProfiles“ verwendet die folgende Syntax:

```
ListDefaultOSProfiles
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-RecipientName|-nm> recipient_name]
[<-RecipientSecurityDomain|-ns> security_domain_of_recipient]
[<-RecipientType|-ty> recipient_type]
[<-IndirectInheritance|-in> indirect_inheritance]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListDefaultOSProfiles“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-RecipientName -nm	recipient_name	Optional. Benutzer- oder Gruppenname, der dem Standardbetriebssystemprofil zugewiesen wird.
-RecipientSecurityDomain -ns	security_domain_of_recipient	Optional. Name der Sicherheitsdomäne, zu der der Benutzer gehört, wenn Sie LDAP-Authentifizierung verwenden.
-RecipientType -ty	recipient_type	Optional. Geben Sie an, ob der Empfänger ein Benutzer oder eine Gruppe ist. Geben Sie einen der folgenden Werte ein: - UserIdentity - GroupIdentity
-IndirectInheritance -in	indirect_inheritance	Optional. Geben Sie einen der folgenden Werte ein: - True. Listet die Betriebssystemprofile auf, die von den Benutzern bzw. Gruppen übernommen wurden. - false. Listet die Betriebssystemprofile auf, die den Benutzern bzw. Gruppen direkt zugewiesen werden.

## ListDomainCiphers

Zeigt eine oder mehrere der folgenden Listen mit Chiffre-Suites an: Blacklist, Standardliste, Gültigkeitsliste oder Whitelist.

Bei der Verwendung von sicherer Kommunikation innerhalb der Domäne und von sicheren Verbindungen mit Webclients zieht Informatica eine Gültigkeitsliste für Chiffre-Suites zur Verschlüsselung von Datenverkehr heran. Informatica ermittelt die Gültigkeitsliste mit Chiffre-Suites auf Grundlage der folgenden Listen:

### Blacklist

Liste mit Chiffre-Suites, die von der Informatica-Domäne blockiert werden sollen. Wenn Sie der Blacklist eine Chiffre-Suite hinzufügen, entfernt die Informatica-Domäne diese Chiffre-Suite aus der Gültigkeitsliste. Sie können Chiffre-Suites, die sich in der Standardliste befinden, zur Blacklist hinzufügen.

### Standardliste

Liste mit Chiffre-Suites, die von der Informatica-Domäne standardmäßig unterstützt werden.

## Whitelist

Liste mit Chiffre-Suites, die von der Informatica-Domäne zusätzlich zu denen in der Standardliste unterstützt werden sollen. Wenn Sie der Whitelist eine Chiffre-Suite hinzufügen, fügt die Informatica-Domäne die Chiffre-Suite zur Gültigkeitsliste hinzu. Chiffre-Suites, die sich in der Standardliste befinden, müssen nicht zur Whitelist hinzugefügt werden.

Mit dem Befehl „ListDomainCiphers“ zeigen Sie die Liste mit Chiffre-Suites an.

Der Befehl „infacmd isp ListDomainCiphers“ verwendet die folgende Syntax:

```
ListDomainCiphers

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-lists|-l> comma_separated_list_of_cipher_configurations...
(ALL,BLACK,WHITE,EFFECTIVE,DEFAULT)]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListDomainCiphers“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
- SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-lists -l	comma_separated_list_of_cipher_configurations	<p>Optional. Kommagetrennte Liste von Argumenten, die die Chiffre-Suites angibt, die Sie anzeigen möchten.</p> <p>Mit dem Argument „ALL“ werden die Blacklist, Standardliste, Gültigkeitsliste und Whitelist angezeigt.</p> <p>Mit dem Argument „BLACK“ wird die Blacklist angezeigt.</p> <p>Mit dem Argument „DEFAULT“ wird die Standardliste angezeigt.</p> <p>Das Argument EFFECTIVE zeigt die Liste der von der Informatica-Domäne unterstützten Chiffre-Suites an.</p> <p>Mit dem Argument „WHITE“ wird die Whitelist angezeigt.</p> <p><b>Hinweis:</b> Bei den Argumenten wird zwischen Groß- und Kleinschreibung unterschieden.</p> <p>Wird bei Ausführung des Befehls auf einem Gateway-Knoten diese Option ausgelassen, werden mit dem Befehl sämtliche Listen mit Chiffre-Suites angezeigt.</p> <p>Wird bei Ausführung des Befehls auf einem Arbeitsknoten diese Option ausgelassen, werden mit dem Befehl die Standardliste und die Gültigkeitsliste mit Chiffre-Suites angezeigt.</p>

## ListDomainLinks

Listet die Domänen auf, mit der die lokale Domäne verknüpft werden kann. Sie stellen Links zwischen zwei Domänen her, wenn Sie Repository-Metadaten zwischen diesen Domänen austauschen möchten.

Der Befehl „infacmd isp ListDomainLinks“ verwendet die folgende Syntax:

```
ListDomainLinks
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```



In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListDomainLinks“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der lokalen Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeitraum in Sekunden, in dem infacmd versucht, eine Verbindung zur lokalen Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

# ListDomainOptions

Listet allgemeine Eigenschaften der Domäne auf. Die Eigenschaften beinhalten Resistenz-Timeout, Grenzwert für Resistenz-Timouts, maximale Neustartversuche, Neustartzeitraum, SSL-Modus und Sendemodus.

Um den infacmd isp ListDomainOptions-Befehl auszuführen, müssen Sie über Berechtigungen für die Domäne verfügen.

Der Befehl „infacmd isp ListDomainOptions“ verwendet die folgende Syntax:

```
ListDomainOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListDomainOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

## ListFolders

Listet die Ordner in der Domäne auf.

Der Befehl „infacmd isp ListFolders“ verwendet die folgende Syntax:

```
ListFolders
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListFolders“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

# ListGridNodes

Listet die einem Gitter zugewiesenen Knoten auf.

Um den `infacmd isp ListGridNodes`-Befehl auszuführen, müssen Sie über Berechtigungen für das Gitter verfügen.

Der Befehl „`infacmd isp ListGridNodes`“ verwendet die folgende Syntax:

```
ListGridNodes

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-GridName|-gn> grid_name
```

In der folgenden Tabelle werden *infacmd isp ListGridNodes* beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GridName -gn	grid_name	Erforderlich. Name des Gitters.

## ListGroupPermissions

Listet Gruppenberechtigungen für ein Objekt auf.

Der Befehl „infacmd isp ListGroupPermissions“ verwendet die folgende Syntax:

```
ListGroupPermissions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingGroup|-eg> existing_group_name
[<-ExistingGroupSecurityDomain|-egn> existing_group_security_domain]
[<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListGroupPermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingGroup -eg	existing_group_name	Erforderlich. Name der Gruppe, der Sie eine Berechtigung für ein Objekt zuweisen möchten.
-ExistingGroupSecurityDomain -egn	existing_group_security_domain_name	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der die Gruppe gehört, der Sie eine Berechtigung zuweisen möchten. Standardwert ist „Native“.
-ObjectType -ot	object_type	Erforderlich. Typ des Objekts, das Sie auflisten möchten: <ul style="list-style-type: none"> <li>- Dienst</li> <li>- License</li> <li>- Knoten</li> <li>- Gitter</li> <li>- Folder</li> <li>- OSProfile</li> </ul>

## ListGroupPrivileges

Listet Berechtigungen auf, die einer Gruppe in der Domäne zugewiesen sind. Sie können ebenfalls Gruppenberechtigungen für jeden Anwendungsdienst in der Domäne zuweisen.

Der Befehl „infacmd isp ListGroupPrivileges“ verwendet die folgende Syntax:

```
ListGroupPrivileges
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GroupName|-gn> group_name
```



[<-GroupSecurityDomain|-gsf> group\_security\_domain]

<-ServiceName|-sn> service\_name

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListGroupPrivileges“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GroupName -gn	group_name	Erforderlich. Name der Gruppe, für die Sie Berechtigungen auflisten möchten.
-GroupSecurityDomain -gsf	group_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der die Gruppe gehört, für die Sie Berechtigungen auflisten möchten. Standardwert ist „Native“.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, für die bzw. den Sie Berechtigungen anzeigen möchten.

## ListGroupsForUser

Listet die nativen Gruppen auf, zu denen der Benutzer zugewiesen ist.

Der infacmd isp-Befehl ListGroupsForUser verwendet folgende Syntax:

```
ListGroupsForUser
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_Name
[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListGroupsForUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_name	Erforderlich. Name des Benutzers, für den Sie Gruppen auflisten möchten.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Standardwert ist „Native“.

## ListLDAPConnectivity

Listet die Details für die angegebene LDAP-Konfiguration auf.

Der Befehl „infacmd isp ListLDAPConnectivity“ verwendet die folgende Syntax:

```
ListLDAPConnectivity
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LDAPHostConfigurationName|-lcn> LDAP_host_configuration_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListLDAPConnectivity“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LDAPHostConfigurationName -lcn	LDAP-Hostkonfigurationsname	Erforderlich. Der Name der LDAP-Konfiguration.

## ListLicenses

Listet die Lizenzen in der Domäne auf. Sie können den Lizenznamen und die Seriennummer für jede Lizenz anzeigen.

Um den infacmd isp ListLicenses-Befehl auszuführen, müssen Sie über Berechtigungen für die Lizenzen verfügen.

Der Befehl „infacmd isp ListLicenses“ verwendet die folgende Syntax:

```
ListLicenses
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port ...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListLicenses“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

# ListMonitoringOptions

Listet allgemeine Überwachungseigenschaften auf.

Der infacmd isp listMonitoringOptions-Befehl verwendet die folgende Syntax:

```
listMonitoringOptions
<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp listMonitoringOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.



Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Anzahl der Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang. Standardwert ist 180 Sekunden.

## ListNodeOptions

Listet die allgemeinen Eigenschaften für einen Knoten auf. Allgemeine Eigenschaften beinhalten das Backup-Verzeichnis, das CPU-Profil, die Fehlerschweregradstufe, maximale und minimale Prozessports und Ressourcenbereitstellungsgrenzen.

Um den infacmd isp ListNodeOptions-Befehl auszuführen, müssen Sie über Berechtigungen für den Knoten verfügen.

Der Befehl „infacmd isp ListNodeOptions“ verwendet die folgende Syntax:

```
ListNodeOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListNodeOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, für den Sie die Optionen auflisten möchten.

# ListNodeResources

Listet alle für einen Knoten definierten Ressourcen auf. Dieser Befehl gibt für jede Ressource den Ressourcentyp zurück und gibt an, ob die Ressource verfügbar ist.

Um den infacmd isp ListNodeResources-Befehl auszuführen, müssen Sie über Berechtigungen für den Knoten verfügen.

Der Befehl „infacmd isp ListNodeResources“ verwendet die folgende Syntax:

```
ListNodeResources

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

[<-ResourceCategory|-rc> resource_category ("PCIS", "DIS")]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListNodeResources“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domännennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domännennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, für den Sie die Ressourcen auflisten möchten.
-ResourceCategory -rc	resource_category	<p>Optional. Kategorie der Ressourcen, die Sie auflisten möchten. Gültige Kategorien umfassen:</p> <ul style="list-style-type: none"> <li>- PCIS. Ressource für den PowerCenter-Integrationsdienst.</li> <li>- DIS. Für zukünftige Verwendung reserviert.</li> </ul> <p>Standardwert ist PCIS.</p>

## ListNodeRoles

Listet alle Rollen auf einem Knoten in der Domäne auf.

Der infacmd isp ListNodeRoles-Befehl verwendet die folgende Syntax:

```
ListNodeRoles
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

[<-ResilienceTimeout|-re> timeout\_period\_in\_seconds]

<-NodeName|-nn> node\_name

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListNodeRoles“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens.

## ListNodes

Listet die Knoten in der Domäne auf. Wenn Sie die Knotenrollenoption nicht verwenden, listet der Befehl alle Knoten in der Domäne auf. Wenn Sie die Knotenrollenoption verwenden, listet der Befehl die Knoten mit der angegebenen Rolle auf.

Der Befehl „infacmd isp ListNodes“ verwendet die folgende Syntax:

```
ListNodes
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-NodeRole|-nr> node_role SERVICE|COMPUTE|SERVICE_COMPUTE]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListNodes“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeRole -nr	node_role	Optional. Aktivierte Rolle für die Knoten, die Sie auflisten möchten. Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- „Service“. Listet Knoten auf, die mindestens über die Dienstrolle verfügen.</li> <li>- „Compute“. Listet Knoten auf, die mindestens über die Berechnungsrolle verfügen.</li> <li>- „Service_compute“. Listet Knoten auf, die über die Dienst- und Berechnungsrolle verfügen.</li> </ul> Wenn Sie die Option nicht angeben, listet der Befehl alle Knoten in der Domäne auf.

## ListOSProfiles

Listet die Betriebssystemprofile in der Domäne auf.

Der Befehl „infacmd isp ListOSProfile“ verwendet die folgende Syntax:

```
ListOSProfiles
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```



In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListOSProfile“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

# ListRepositoryLDAPConfiguration

Listet die LDAP-Serverkonfigurationsoptionen wie LDAP-Serveradresse, Suchbereich und Anmeldeattribute auf.

Verwenden Sie nach dem Installieren von Informatica diesen Befehl, um die Verbindung zwischen der Domäne und dem externen LDAP-Verzeichnisdienst zu überprüfen.

Verwenden Sie `infacmd isp SetRepositoryLDAPConfiguration`, um die LDAP-Serverkonfigurationsoptionen für eine Informatica-Domäne zu aktualisieren. Verwenden Sie diesen Befehl, wenn Sie ein Repository aktualisieren, das LDAP-Authentifizierung verwendet.

Der Befehl „`infacmd isp ListRepositoryLDAPConfiguration`“ verwendet die folgende Syntax:

```
ListRepositoryLDAPConfiguration
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd isp ListRepositoryLDAPConfiguration`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

## ListRolePrivileges

Listet Berechtigungen auf, die einer Rolle in der Domäne zugewiesen sind. Sie können ebenfalls Rollenberechtigungen für jeden Anwendungsdienst in der Domäne auflisten.

Sie können einer Rolle zugewiesene Berechtigungen für die Domäne und für jeden Anwendungsdiensttyp in der Domäne auflisten.

Der Befehl „infacmd isp ListRolePrivileges“ verwendet die folgende Syntax:

```
ListRolePrivileges
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

<-RoleName|-rn> role\_name

In der folgenden Tabelle werden die Optionen und Argumente für „ListRolePrivileges“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RoleName -rn	role_name	Erforderlich. Name der Rolle, für die Berechtigungen aufgelistet werden. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

## ListSecurityDomains

Listet die nativen und LDAP-Sicherheitsdomänen in der Domäne auf.

Der Befehl „infacmd isp ListSecurityDomains“ verwendet die folgende Syntax:

```
ListSecurityDomains
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListSecurityDomains“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

# ListServiceLevels

Listet die Dienstebenen auf, die für die Domäne definiert sind. Sie können den Namen, die Dispatch-Priorität und die maximale Dispatch-Wartezeit für jede Dienstebene auflisten.

Der Befehl „infacmd isp ListServiceLevels“ verwendet die folgende Syntax:

```
ListServiceLevels  
  
<-DomainName|-dn> domain_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-SecurityDomain|-sdn> security_domain]  
  
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListServiceLevels“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

## ListServiceNodes

Listet die Knoten oder Gitter auf, die einem Dienst zugewiesen sind.

Wenn dieser Befehl einen Gitternamen zurückgibt, können Sie den infacmd isp ListGridNodes-Befehl ausführen, um die Knoten in einem Gitter aufzulisten.

Um den infacmd isp ListServiceNodes-Befehl auszuführen, müssen Sie über Berechtigungen für den Dienst verfügen.

Der Befehl „infacmd isp ListServiceNodes“ verwendet die folgende Syntax:

```
ListServiceNodes
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
```



In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListServiceNodes“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Diensts.

#### VERWANDTE THEMEN:

- [“ListGridNodes” auf Seite 633](#)

## ListServicePrivileges

Listet die Berechtigungen für eine Domäne oder einen Anwendungsdiensttyp auf.

Der Befehl „infacmd isp ListServicePrivileges“ verwendet die folgende Syntax:

```
ListServicePrivileges
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-ServiceType|-st> service_type AS|CMS|LDM|MM|MRS|RS|TDM|TDW|DOMAIN]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListServicePrivileges“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceType -st	service_type	Optional. Domäne oder Anwendungsdiensttyp, für die bzw. den Sie Berechtigungen anzeigen möchten.  Zu den Dienstypen gehören: <ul style="list-style-type: none"> <li>- AS. Analyst-Dienst</li> <li>- CMS. Content-Managementdienst</li> <li>- CS. Katalogdienst</li> <li>- MM. Metadata Manager-Dienst</li> <li>- MRS. Modellrepository-Dienst</li> <li>- RS. PowerCenter-Repository-Dienst</li> <li>- TDM. Test Data Manager-Dienst</li> <li>- TDW. Test Data Warehouse-Dienst</li> <li>- DOMAIN. Domäne</li> </ul>

## ListServices

Listet die Dienste in der Domäne auf.

Der Befehl „infacmd isp ListServices“ verwendet die folgende Syntax:

```
ListServices

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-ServiceType|-st> service_type AS|BW|CMS|DIS|ES|IHS|IS|LDM|MM|MRS|RMS|RS|SCH|SEARCH|
TDM|TDW|WS]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListServices“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port .. .	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceType -st	service_type	Optional. Listet alle Dienste eines bestimmten Typs auf. Zu den Diensttypen gehören: <ul style="list-style-type: none"> <li>- AS. Analyst-Dienst</li> <li>- BW. SAP BW-Dienst</li> <li>- CMS. Content-Managementdienst</li> <li>- DIS. Datenintegrationsdienst</li> <li>- ES. E-Mail-Dienst</li> <li>- IHS. Informatica-Cluster-Dienst</li> <li>- IS. PowerCenter-Integrationsdienst</li> <li>- CS. Katalogdienst</li> <li>- MM. Metadata Manager-Dienst</li> <li>- MRS. Modellrepository-Dienst</li> <li>- RMS. Ressourcenmanager-Dienst</li> <li>- RS. PowerCenter-Repository-Dienst</li> <li>- SCH. Scheduler-Dienst</li> <li>- SEARCH. Suchdienst</li> <li>- TDM. Test Data Manager-Dienst</li> <li>- TDW. Test Data Warehouse-Dienst</li> <li>- WS. Webdienst-Hub</li> </ul>

## ListSMTPOptions

Listet die SMTP-Konfigurationseigenschaften für die Domäne auf. Die SMTP-Konfiguration dient zum Senden von Domänenwarnungen und Scorecard-Benachrichtigungen.

Der Befehl „infacmd isp ListSMTPOptions“ verwendet die folgende Syntax:

```
ListSMTPOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListSMTPOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

## VERWANDTE THEMEN:

- [“UpdateSMTPOptions” auf Seite 813](#)

# ListUserPermissions

Listet die Domänenobjekte auf, für die ein Benutzer Berechtigungen hat.

Der Befehl „`infacmd isp ListUserPermissions`“ verwendet die folgende Syntax:

```
ListUserPermissions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_name

[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]

[<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE]
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd isp ListUserPermissions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.



Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_name	Erforderlich. Benutzerkonto, für das Sie Berechtigungen auflisten möchten. Um einen Namen einzugeben, der Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

Option	Argument	Beschreibung
-ExistingUserSecurityDomain -esd	existing_user_security_do mainth_name	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, für den Sie Berechtigungen auflisten möchten. Standardwert ist „Native“.
-ObjectType -ot	object_type	Erforderlich. Typ des Objekts, das Sie auflisten möchten: <ul style="list-style-type: none"> <li>- Dienst</li> <li>- License</li> <li>- Knoten</li> <li>- Gitter</li> <li>- Folder</li> <li>- OSPProfile</li> </ul>

## ListUserPrivileges

Listet Berechtigungen auf, die einem Benutzer in der Domäne zugewiesen sind. Sie können ebenfalls Benutzerberechtigungen für jeden Anwendungsdienst in der Domäne auflisten.

Der Befehl „infacmd isp ListUserPrivileges“ verwendet die folgende Syntax:

```
ListUserPrivileges
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_Name
[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListUserPrivileges“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
ExistingUserName -eu	existing_user_name	Erforderlich. Benutzerkonto, für das Sie Berechtigungen auflisten möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, für den Sie Berechtigungen auflisten möchten. Standardwert ist „Native“.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, für die bzw. den Sie Berechtigungen anzeigen möchten.

## infacmd ListWeakPasswordUsers

Listet die Benutzer mit Passwörtern auf, die die Passwortrichtlinie nicht erfüllen.

Der Befehl „infacmd ListWeakPasswordUsers“ verwendet die folgende Syntax:

```
ListWeakPasswordUsers
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für infacmd ListWeakPasswordUsers beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Geben Sie die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne an.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang. Standardwert ist 180 Sekunden.

# migrateUsers

Migriert die Gruppen, Rollen, Rechte und Berechtigungen der Benutzer in der nativen Sicherheitsdomäne für Benutzer auf eine oder mehrere LDAP-Sicherheitsdomänen. Bevor Sie eine Domäne zur Verwendung von Kerberos-Authentifizierung konfigurieren, müssen Sie die Benutzer auf eine LDAP-Sicherheitsdomäne migrieren.

Weitere Informationen zum Befehl „migrateUsers“ finden Sie im *Informatica-Sicherheitshandbuch*.

Der Befehl „infacmd isp migrateUsers“ verwendet die folgende Syntax:

```
migrateUsers

<-DomainName|-dn> domain_name

<-UserName|-un> administrator_user_name

<-Password|-pd> administrator_password

[<-SecurityDomain|-sdn>|security_domain]

[<-Gateway|-hp>|gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds ]

<-UserMigrationFile|-umf> user_migration_file
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp migrateUsers“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	administrator_user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	administrator_password	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Optional. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. <b>Hinweis:</b> Diese Sicherheitsdomäne ist die Sicherheitsdomäne des Benutzerkontos, das zum Herstellen einer Verbindung zur Domäne verwendet wird, nicht zur Sicherheitsdomäne, auf die die Benutzer migriert werden.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Optional. Verwenden, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-UserMigrationFile -umf	user_migration_file	Erforderlich. Pfad und Dateiname der Benutzermigrationsdatei. Die Benutzermigrationsdatei ist eine Textdatei, die die Liste der nativen Benutzer und die entsprechenden LDAP-Benutzer enthält. Einträge müssen im folgenden Format vorliegen:  Native/<SourceUserName>,LDAP/<TargetUsername>  Beispiel: Um einen Benutzer namens Benutzer1 aus der nativen Sicherheitsdomäne in einen Benutzer namens Benutzer1 in einer LDAP-Sicherheitsdomäne zu migrieren, fügen Sie der Benutzermigrationsdatei die folgende Zeile hinzu:  Native/User1,LDAP/User1  Der Befehl überspringt Einträge mit einem doppelten Quell- oder Zielbenutzernamen.

## MoveFolder

Entfernt einen Ordner.

Der Befehl „infacmd isp MoveFolder“ verwendet die folgende Syntax:

```
MoveFolder
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-OriginalPath|-op> original_folder_path
<-FolderPath|-fp> full_folder_path
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp MoveFolder“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.



Option	Argument	Beschreibung
-OriginalPath -op	original_folder_path	Erforderlich. Vollständiger Pfad (ohne Domänenname) des zu verschiebenden Ordners. Folgendes Format ist erforderlich: <i>/parent_folder/child_folder</i>
-FolderPath -fp	full_folder_path	Erforderlich. Vollständiger Pfad (ohne Domänenname) zum Speicherort des Zielordners. Folgendes Format ist erforderlich: <i>/parent_folder/child_folder</i>

## MoveObject

Verschiebt ein Objekt in einen anderen Ordner.

Der Befehl „infacmd isp MoveObject“ verwendet die folgende Syntax:

```
MoveObject
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ObjectName|-on> object_name
<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID
<-FolderPath|-fp> full_folder_path
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp MoveObject“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ObjectName -on	object_name	Erforderlich. Name des Objekts, das Sie verschieben möchten.

Option	Argument	Beschreibung
-ObjectType -ot	object_type	Erforderlich. Typ des Objekts, das Sie verschieben möchten: <ul style="list-style-type: none"> <li>- Dienst</li> <li>- Lizenz</li> <li>- Knoten</li> <li>- Gitter</li> </ul>
-FolderPath -fp	full_folder_path	Erforderlich. Vollständiger Pfad (ohne Domänenname) des Ordners, in den Sie das Objekt verschieben möchten. Folgendes Format ist erforderlich:  <code>/parent_folder/child_folder</code>

## Ping

Pingt eine Domäne, einen Dienst, einen Domänen-Gateway-Host oder einen Knoten. Wenn das Objekt verfügbar ist, zeigt dieser Befehl eine Meldung an, dass das Objekt an einem bestimmten Port auf dem Gateway-Host-Computer verfügbar ist. Wenn das Objekt nicht verfügbar ist, zeigt dieser Befehl eine Meldung darüber an, dass keine Antwort von der Domäne empfangen wurde.

Verwenden Sie diesen Befehl zur Fehlerbehebung von Netzwerkverbindungen. Um den infacmd isp Ping-Befehl auszuführen, müssen Sie über Berechtigungen für das Objekt verfügen, das Sie pingen möchten.

Der infacmd isp Ping-Befehl zeigt keine Ergebnisse für einzelne Dienstprozesse an.

Der infacmd isp Ping-Befehl verwendet die folgende Syntax:

```
Ping
[<-DomainName|-dn> domain_name]
[<-ServiceName|-sn> service_name]
[<-GatewayAddress|-dg> domain_gateway_host:port]
[<-NodeName|-nn> node_name]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden infacmd isp Ping-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domännennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domännennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Optional. Name des Diensts, den Sie anpingen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

Option	Argument	Beschreibung
-GatewayAddress -dg	domain_gateway_host:port	Erforderlich, wenn Sie die Option -DomainName nicht angeben oder wenn Sie eine andere Domäne anpingen müssen. Name und Portnummer des Gateway-Hostcomputers.
-NodeName -nn	node_name	Optional. Name des Knotens.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

## PingDomain

Pingt alle Knoten und Dienste in einer Domäne. Zeigt den Status der Domäne, der Knoten und der Dienste an. Sie können die Ausgabe in eine Text-oder CSV-Datei schreiben.

Die Ausgabe verwendet die folgenden Formate, um den Status der Domäne, der Knoten und der Dienste anzuzeigen:

- Domäne. MASTER\_NODE\_NAME, STATUS, HOST:PORT.
- Knoten. DOMAIN\_NAME, NODE\_NAME, STATUS, HOST:PORT.
- Service. SERVICE\_NAME, NODE\_NAME, STATUS, HOST:PORT.

Wenn ein Dienst in der Domäne deaktiviert ist, wird der Status DISABLED angezeigt. Die Ausgabe zeigt weder Knotennamen noch Hostnamen oder Portnummer an.

Wenn der Dienst in einem Gitter ausgeführt wird, pingt der Befehl jeden Knoten im Gitter. Die Ausgabe zeigt den Status des Diensts auf jedem Knoten an.

Der Befehl „infacmd isp PingDomain“ verwendet die folgende Syntax:

```
PingDomain

[<-DomainName|-dn> domain_name]

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-Format|-fm> format_TEXT_CSV]

[<-OutputFile|-of> output_file_name]
```

In der folgenden Tabelle werden die Optionen und Argumente für infacmd isp PingDomain beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-Format -fm	format_TEXT_CSV	Optional. Format zur Anzeige des Domänen-, Knoten- und Dienststatus. Sie können TEXT oder CSV angeben. Das Standardformat ist TEXT.
-OutputFile -of	output_file_name	Name und Dateipfad für die Erstellung der Ausgabedatei.

## PrintSPNAndKeytabNames

Generiert die Liste der SPN- und Keytab-Dateinamen für die Knoten und Dienste in der Domäne. In der Informatica-Domäne muss jeder SPN eine Keytab-Datei enthalten. Sie müssen unter Umständen den Kerberos-Administrator bitten, die SPNs zur Prinzipaldatenbank hinzuzufügen und die Keytab-Dateien zu erstellen. Die SPNs und Keytab-Dateinamen unterliegen der Groß-/Kleinschreibung.

Der Befehl „`infacmd isp PrintSPNAndKeytabNames`“ verwendet die folgende Syntax:

```
PrintSPNAndKeytabNames

<-DomainName|-dn> domain_name

<-ServiceRealmName|-srn> realm_name_of_node_spn

[<-Format|-fm> format_TEXT_CSV]

[<-OutputFile|-of> output_file_name]

[<-DomainNodes|-dns> Node1:HostName1 Node2:HostName2 ...]

[<-ServiceProcesses|-sps> ServiceName1:NodeName1 ServiceName2:NodeName2...]

[<-SPNShareLevel|-spnSL> SPNShareLevel PROCESS|NODE]
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd isp PrintSPNAndKeytabNames`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceRealmName -srn	realm_name_of_node_spn	Erforderlich. Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Der Bereichsname muss in Großbuchstaben angegeben werden und die Groß-/Kleinschreibung wird unterschieden.
-Format -fm	format_TEXT_CSV	Optional. Format der Ausgabedatei. Gültige Typen umfassen: - Text - CSV  Wenn Sie kein Format angeben, verwendet infacmd Textformat mit einer Zeilenlänge von 80 Zeichen.

Option	Argument	Beschreibung
-OutputFile -of	output_file_name	Optional. Name und Dateipfad für die Ausgabedatei. Wenn Sie keinen Ausgabedateinamen angeben, zeigt infacmd die Protokollereignisse auf dem Bildschirm an.
-DomainNodes -dns	NodeName:HostName [NodeName:Hostname ]	Name des Knotens und der voll qualifizierte Hostname des Computers, der den Knoten hostet. Verwenden Sie das folgende Format: NodeName:HostName  Sie können SPNs und Keytab-Dateinamen für mehrere Knoten generieren. Trennen Sie jedes Knotennamen- und Hostnamen-Paar mit einem Leerzeichen.
-ServiceProcesses -sps	ServiceName:NodeName [ServiceName:Knotenname]	Optional. Name des Diensts, den Sie in der Informatica-Domäne erstellen möchten, sowie der Name des Knotens, auf dem der Dienst ausgeführt werden soll. Verwenden Sie das folgende Format: ServiceName:NodeName  Sie können SPNs und Keytab-Dateinamen für mehrere Dienste generieren. Trennen Sie jedes aus Dienst- und Knotenname bestehende Paar durch ein Leerzeichen.  <b>Hinweis:</b> Die Schlüsseltabellen-Dateien für Anwendungsdienste in der Domäne müssen für die Konfiguration der Domäne zwecks Kerberos-Authentifizierung nicht verfügbar sein. Sie können den Dienst-SPN zur Prinzipaldatenbank hinzufügen und die Schlüsseltabelle erstellen, nachdem Sie die Authentifizierung der Informatica-Domäne geändert haben, bevor Sie jedoch den Dienst aktivieren.
SPNShareLevel -spnSL	SPNShareLevel PROCESS[NODE]	Optional. Gibt die Dienst-Prinzipalebene für die Domäne an. Legen Sie eine der folgenden Ebenen für die Eigenschaft fest: <ul style="list-style-type: none"> <li>- Prozess Die Domäne erfordert einen eindeutigen Dienst-Prinzipalnamen (SPN) und eine Keytab-Datei für jeden Knoten und für jeden Dienst auf einem Knoten. Die Anzahl der für jeden Knoten erforderlichen SPNs und Keytab-Dateien hängt von der Anzahl der Dienstprozesse ab, die auf dem Knoten ausgeführt werden. Empfohlen für Produktionsdomänen.</li> <li>- Knoten. Die Domäne verwendet einen SPN und eine Keytab-Datei für den Knoten und für alle Dienste, die auf dem Knoten ausgeführt werden. Sie erfordert außerdem einen separaten SPN und eine separate Keytab-Datei für alle HTTP-Prozesse auf dem Knoten. Empfohlen für Test- und Entwicklungsdomänen. Empfohlen für Test- und Entwicklungsdomänen.</li> </ul> Standardwert ist „Prozess“.

## PurgeLog

Bereinigt Protokollereignisse. Sie können Protokollereignisse für eine Domäne oder für Anwendungsdienste löschen, wie zum Beispiel der PowerCenter-Integrationsdienst, der Datenintegrationsdienst und der Webdienst-Hub.

Der Befehl „infacmd isp PurgeLog“ verwendet die folgende Syntax:

```
PurgeLog
<-DomainName|-dn> domain_name
```

```

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-BeforeDate|-bd> before_date

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp PurgeLog“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.



Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-BeforeDate -bd	before_date	Erforderlich. Bereinigt Protokollereignisse, die vor diesem Datum und dieser Uhrzeit aufgetreten sind. Geben Sie Datum und Uhrzeit in einem der folgenden Formate ein: - MM/dd/yyyy - jjjj-MM-tt

## PurgeMonitoringData

Bereinigt Überwachungsdaten im Modellrepository.

Der Befehl `purgeMonitoringData` verwendet folgende Syntax:

```
<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-NumDaysToRetain|-ndr> num_days_to_retain]

[<-NumDaysToRetainDetailedStat|-ndrds> num_days_to_retain_detailed_stat]
```

In der folgenden Tabelle werden die Optionen und Argumente von „purgeMonitoringData“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne des Benutzers. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei <code>domains.infa</code> veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Anzahl der Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option <code>-re</code> oder der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option <code>-re</code> Vorrang. Standardwert ist 180 Sekunden.
-NumDaysToRetain -ndr	num_days_to_retain	Optional. Anzahl der Tage, die gemittelte Daten im Modellrepository beibehalten werden.  Wenn Sie beispielsweise 180 eingeben, bereinigt der Modellrepository-Dienst alle gemittelten Daten, die älter als 180 Tage sind. Minimalwert ist 0. Maximalwert ist 366.  Die Option <code>-ndr</code> verwendet standardmäßig den Wert der Option <b>Zusammengefasste historische Daten beibehalten</b> aus der Überwachungskonfiguration.
-NumDaysToRetainDetailedStat -ndrds	num_days_to_retain_detailed_stat	Optional. Anzahl der Tage, die minutengenaue Daten im Modellrepository beibehalten werden.  Wenn Sie beispielsweise 7 eingeben, bereinigt der Modellrepository-Dienst alle gemittelten Daten, die älter als 7 Tage sind. Minimalwert ist 0. Maximalwert ist 14.  Die Option <code>-ndrds</code> verwendet standardmäßig den Wert der Option <b>Detaillierte historische Daten beibehalten</b> aus der Überwachungskonfiguration.

## RemoveAlertUser

Hebt das Abonnement von Alarm-E-Mail-Nachrichten für einen Benutzer auf. Sie können infacmd isp RemoveAlertUser für alle Benutzer ausführen.

Der Befehl „infacmd isp RemoveAlertUser“ verwendet die folgende Syntax:

```
RemoveAlertUser
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
```

```

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-AlertUser|-au> user_name

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveAlertUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-AlertUser -au	user_name	Erforderlich. Name des Benutzers, für den Sie das Abonnement von Alarmen aufheben möchten.

## RemoveConnection

Entfernt eine Verbindung aus der Domäne.

Der Befehl „infacmd isp RemoveConnection“ verwendet die folgende Syntax:

```
RemoveConnection
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConnectionName|-cn> connection_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveConnection“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ConnectionName -cn	connection_name	Name der zu entfernenden Verbindung.

## RemoveConnectionPermissions

Entfernt Verbindungsberechtigungen für einen Benutzer oder eine Gruppe.

Der Befehl „infacmd isp RemoveConnectionPermissions“ verwendet die folgende Syntax:

```
RemoveConnectionPermissions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<<-RecipientUserName|-run> recipient_user_name|<ReceipeintGroupName|-rgn>
recipeint_group_name>
<-RecipientSecurityDomain|-rsd> recipient_security_domain]
<-ConnectionName|-cn> connection_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveConnectionPermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.



Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RecipientUserName -run	recipient_user_name	Erforderlich, wenn Sie den Gruppennamen des Empfängers nicht angeben. Name des Benutzers, für den Berechtigungen entfernt werden.
-RecipientGroupName -rgn	recipient_group_name	Erforderlich, wenn Sie den Benutzernamen des Empfängers nicht angeben. Name der Gruppe, für die Berechtigungen für die Verbindung entfernt werden.
-RecipientSecurityDomain -rsd	recipient_security_domain_name	Erforderlich, wenn der Empfänger zu einer LDAP-Sicherheitsdomäne gehört. Name der Sicherheitsdomäne, zu der der Empfänger gehört. Standardwert ist „Native“.
-ConnectionName -cn	connection_name_security_domain	Erforderlich. Name der Verbindung.

## removeCustomLDAPType

Entfernt den angegebenen benutzerdefinierten LDAP-Typ.

Der Befehl „infacmd isp removeCustomLDAPType“ verwendet die folgende Syntax:

```
removeCustomLDAPType
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-CustomLDAPTypeName|-lt> custom_LDAP_type_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp removeCustomLDAPType“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-CustomLDAPTypeName -lt	Name des benutzerdefinierten LDAP-Typs	Erforderlich. Der Name des zu entfernenden benutzerdefinierten LDAP-Typs.

## RemoveDomainLink

Entfernt eine verknüpfte Domäne. Wenn Sie eine verknüpfte Domäne entfernen, können Sie keine Repository-Metadaten zwischen der lokalen und der verknüpften Domäne herstellen. Möglicherweise gehen Sie so vor, wenn Sie in einer anderen Domäne nicht mehr auf den PowerCenter-Repository-Dienst zugreifen müssen.

Der Befehl „infacmd isp RemoveDomainLink“ verwendet die folgende Syntax:

```
RemoveDomainLink
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LinkedDomainName|-ld> linked_domain_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveDomainLink“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der lokalen Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeitraum in Sekunden, in dem infacmd versucht, eine Verbindung zur lokalen Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LinkedDomainName -ld	linked_domain_name	Erforderlich. Name der Domäne, aus der Sie eine Verbindung entfernen möchten.

## RemoveFolder

Entfernt alle Ordner aus der Domäne. Bevor Sie einen Ordner entfernen, müssen Sie sicherstellen, dass der Ordner leer ist.

Der Ordner muss leer sein.

Der Befehl „infacmd isp RemoveFolder“ verwendet die folgende Syntax:

```
RemoveFolder
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-FolderPath|-fp> full_folder_path
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveFolder“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-FolderPath -fp	full_folder_path	Erforderlich. Vollständiger Pfad (ohne Domänenname) des zu entfernenden Ordners. Folgendes Format ist erforderlich: <i>/parent_folder/child_folder</i>

## RemoveGrid

Entfernt ein Gitter aus der Domäne. Bevor Sie ein Gitter entfernen können, müssen Sie die Zuweisung des Gitters aus dem PowerCenter Integration Service oder dem Data Integration Service aufheben.

Der infacmd isp RemoveGrid-Befehl verwendet die folgende Syntax:

```
RemoveGrid
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GridName|-gn> grid_name
```

In der folgenden Tabelle werden infacmd isp RemoveGrid-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.

Option	Argument	Beschreibung
-Password -pd	passwort	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -pd festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GridName -gn	grid_name	Erforderlich. Name des Gitters, das Sie entfernen möchten.

## RemoveGroup

Entfernt eine Gruppe aus der nativen Sicherheitsdomäne.

Der Befehl „infacmd isp RemoveGroup“ verwendet die folgende Syntax:

```
RemoveGroup
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```



[<-ResilienceTimeout|-re> timeout\_period\_in\_seconds]

<-GroupName|-gn> group\_name

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveGroup“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GroupName -gn	group_name	Erforderlich. Name der Gruppe, die Sie entfernen möchten.

## RemoveGroupPermission

Entfernt eine Gruppenberechtigung für ein Objekt.

Der Befehl „infacmd isp RemoveGroupPermission“ verwendet die folgende Syntax:

```
RemoveGroupPermission
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingGroup|-eg> existing_group_name
[<-GroupSecurityDomain|-gsf> group_security_domain]
<-ObjectName|-on> object_name
<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveGroupPermission“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingGroup -eg	existing_group_name	Erforderlich. Name der Gruppe, der Sie eine Berechtigung für ein Objekt zuweisen möchten.
-GroupSecurityDomain -gsf	group_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der die Gruppe gehört, der Sie eine Berechtigung zuweisen möchten. Standardwert ist „Native“.
-ObjectName -on	object_name	Name des Objekts, dem Sie die Gruppenzugriffsberechtigung entziehen möchten.
-ObjectType -ot	object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE	Erforderlich. Typ des Objekts Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- Dienst</li> <li>- License</li> <li>- Knoten</li> <li>- Gitter</li> <li>- Folder</li> <li>- OSPProfile</li> </ul>

## RemoveGroupPrivilege

Entfernt eine Berechtigung aus einer Gruppe in der Domäne. Sie können eine Berechtigung aus einer Gruppe für die Domäne oder einen Anwendungsdienst in der Domäne entfernen.

Der Befehl „infacmd isp RemoveGroupPrivilege“ verwendet die folgende Syntax:

```
RemoveGroupPrivilege
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```

<-GroupName|-gn> group_name

[<-GroupSecurityDomain|-gsf> group_security_domain]

<-ServiceName|-sn> service_name

<-PrivilegePath|-pp> path_of_privilege

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveGroupPrivilege“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GroupName -gn	group_name	Erforderlich. Name der Gruppe, aus der Sie die Berechtigung entfernen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-GroupSecurityDomain -gsf	group_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der die Gruppe gehört, aus der Sie Berechtigungen entfernen. Standardwert ist „Native“.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, für die bzw. den Sie Berechtigungen anzeigen möchten.
-PrivilegePath -pp	path_of_privilege	Erforderlich. Vollqualifizierter Name der Berechtigung, die Sie der Gruppe zuweisen möchten. Ein vollqualifizierter Name enthält den Namen der Berechtigungsgruppe und den Namen der Berechtigung. Ein vollqualifizierter Berechtigungsname für den Repository-Dienst ist z. B. „folder/create“. Wenn der Berechtigungsname Leerzeichen enthält, setzen Sie den Pfad wie folgt in Anführungszeichen:  "Runtime Objects/Monitor/Execute/Manage Execution"  Wenn der Berechtigungsname das Sonderzeichen „/“ enthält, fügen Sie das Escape-Zeichen „\“ davor folgendermaßen ein:  "Model/View Model/Export\Import Models"

## removeLDAPConnectivity

Entfernt die angegebene LDAP-Konfiguration.

Der Befehl „infacmd isp removeLDAPConnectivity“ verwendet die folgende Syntax:

```
removeLDAPConnectivity
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
```

```
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
<-LDAPHostConfigurationName|-lcn> LDAP_host_configuration_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp removeLDAPConnectivity“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LDAPHostConfigurationName -lcn	LDAP-Hostkonfigurationsname	Erforderlich. Der Name der zu entfernenden LDAP-Konfiguration.

## RemoveLicense

Entfernt eine Lizenz aus der Domäne. Bevor Sie diesen Befehl ausführen, müssen Sie zuerst die der Lizenz zugewiesenen Dienste deaktivieren.

Entfernt eine Lizenz aus einer Domäne, wenn sie abläuft oder wenn Sie die Lizenz in eine andere Domäne verschieben möchten.

Der Befehl „infacmd isp RemoveLicense“ verwendet die folgende Syntax:

```
RemoveLicense
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LicenseName|-ln> license_name
```



In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveLicense“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz, die Sie entfernen möchten.

## VERWANDTE THEMEN:

- [“DisableService” auf Seite 544](#)
- [“UnassignLicense” auf Seite 754](#)

# RemoveNode

Entfernt alle Knoten aus der Domäne. Wenn der Knoten ausgeführt wird, müssen Sie ihn zunächst herunterfahren.

Der Befehl „infacmd isp RemoveNode“ verwendet die folgende Syntax:

```
RemoveNode

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveNode“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domännennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domännennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, den Sie entfernen möchten.

## RemoveNodeResource

Entfernt eine Ressource aus dem Knoten. Sie können eine benutzerdefinierte Ressource oder eine Datei- bzw. Verzeichnisressource aus einem Knoten entfernen. Sie können keine Verbindungsressource aus einem Knoten entfernen.

Wenn ein PowerCenter-Integrationsdienst in einem Gitter ausgeführt wird, kann der Load Balancer Ressourcen verwenden, um Sitzungs-, Befehls- und vordefinierte Event-Wait-Aufgaben zu verteilen. Wenn der PowerCenter-Integrationsdienst für die Überprüfung von Ressourcen konfiguriert ist, verteilt der Load Balancer Aufgaben an Knoten, auf denen Ressourcen hinzugefügt und aktiviert werden. Wenn Sie eine Ressource entfernen, die von der Sitzungs- oder Befehlsaufgabe benötigt wird, kann die Aufgabe auf diesem Knoten nicht länger ausgeführt werden.

Der Befehl „infacmd isp RemoveNodeResource“ verwendet die folgende Syntax:

```
RemoveNodeResource
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

[<-ResourceCategory|-rc> resource_category ("PCIS", "DIS")]

<-ResourceType|-rt> resource_type("Custom", "File Directory")

<-ResourceName|-rn> resource_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveNodeResource“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens mit der Ressource, die Sie entfernen möchten.
-ResourceCategory -rc	resource_category	Optional. Kategorie der Ressource, die Sie entfernen möchten. Gültige Kategorien umfassen: - PCIS. Ressource für den PowerCenter-Integrationsdienst. - DIS. Für zukünftige Verwendung reserviert. Standardwert ist PCIS.
-ResourceType -rt	resource_type	Erforderlich. Typ der Ressource, die Sie entfernen möchten. Gültige Typen umfassen: - Benutzerdefiniert - Dateiverzeichnis
-ResourceName -rn	resource_name	Erforderlich. Vollständiger Name der zu entfernenden Ressource. Um die Namen aller für einen Knoten verfügbaren Ressourcen aufzulisten, führen Sie den infacmd isp ListNodeResources-Befehl aus.

## RemoveOSProfile

Entfernt ein Betriebssystemprofil aus der Domäne.

Der Befehl „infacmd isp RemoveOSProfile“ verwendet die folgende Syntax:

```
RemoveOSProfile
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-OSProfileName|-on> OSProfile_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveOSProfile“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-OSProfileName -on	OSProfile_name	Erforderlich. Name des Betriebssystemprofils, das Sie entfernen möchten.

## RemoveRole

Entfernt eine benutzerdefinierte Rolle aus der Domäne. Wenn Sie eine benutzerdefinierte Rolle entfernen, werden die benutzerdefinierte Rolle und alle damit verbundenen Berechtigungen für alle Benutzer und Gruppen entfernt, die der Rolle zugewiesen sind.

Der Befehl „infacmd isp RemoveRole“ verwendet die folgende Syntax:

```
RemoveRole
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-RoleName|-rn> role_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveRole“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RoleName -rn	role_name	Erforderlich. Name der Rolle, die Sie entfernen möchten.



# RemoveRolePrivilege

Entfernt eine Berechtigung aus einer Rolle in der Domäne oder aus einer Rolle im Anwendungsdienst innerhalb der Domäne.

Der Befehl „infacmd isp RemoveRolePrivilege“ verwendet die folgende Syntax:

```
RemoveRolePrivileges
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-RoleName|-rn> role_name
<-ServiceType|-st> service_type AS|CMS|LDM|MM|MRS|RS|TDM|TDW|DOMAIN]
<-PrivilegePath|-pp> path_of_privilege
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveRolePrivilege“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RoleName -rn	role_name	Erforderlich. Name der Rolle, aus der Sie die Berechtigung entfernen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

Option	Argument	Beschreibung
-ServiceType -st	service_type	<p>Erforderlich. Domäne oder Anwendungsdiensttyp, aus der bzw. dem Sie die Berechtigung für die Rolle entfernen möchten.</p> <p>Zu den Diensttypen gehören:</p> <ul style="list-style-type: none"> <li>- AS. Analyst-Dienst</li> <li>- CMS. Content-Managementdienst</li> <li>- CS. Katalogdienst</li> <li>- MM. Metadata Manager-Dienst</li> <li>- MRS. Modellrepository-Dienst</li> <li>- RS. PowerCenter-Repository-Dienst</li> <li>- TDM. Test Data Manager-Dienst</li> <li>- TDW. Test Data Warehouse-Dienst</li> <li>- DOMAIN. Domäne</li> </ul>
-PrivilegePath -pp>	path_of_privilege	<p>Erforderlich. Vollqualifizierter Name der Berechtigung, die Sie der Gruppe zuweisen möchten. Ein vollqualifizierter Name enthält den Namen der Berechtigungsgruppe und den Namen der Berechtigung. Ein vollqualifizierter Berechtigungsname für den Repository-Dienst ist z. B. „folder/create“. Wenn der Berechtigungsname Leerzeichen enthält, setzen Sie den Pfad wie folgt in Anführungszeichen:</p> <p>“Runtime Objects/Monitor/Execute/Manage Execution”</p> <p>Wenn der Berechtigungsname das Sonderzeichen „/“ enthält, fügen Sie das Escape-Zeichen „\“ davor folgendermaßen ein:</p> <p>“Model/View Model/Export\Import Models”</p>

## RemoveService

Entfernt einen Anwendungsdienst aus der Domäne. Bevor Sie einen Dienst entfernen, müssen Sie ihn deaktivieren.

Der Befehl „infacmd isp RemoveService“ verwendet die folgende Syntax:

```
RemoveService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, den Sie entfernen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

## RemoveServiceLevel

Entfernt eine Dienstebene. Wenn Sie eine Dienstebene entfernen, aktualisiert der Workflow Manager keine Aufgaben, die die Dienstebene verwenden. Wenn eine Arbeitsablauf-Dienstebene in der Domäne nicht vorhanden ist, sendet der Load Balancer die Aufgaben mit einer Standarddienstebene.

Der Befehl „infacmd isp RemoveServiceLevel“ verwendet die folgende Syntax:

```
RemoveServiceLevel
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceLevelName|-ln> service_level_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveServiceLevel“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceLevelName -ln	service_level_name	Erforderlich. Name der Dienstebene, die Sie entfernen möchten.

## RemoveUser

Entfernt ein Benutzerkonto aus der nativen Sicherheitsdomäne. Benutzerkonten können nicht aus LDAP-Sicherheitsdomänen entfernt werden.

Der Befehl „infacmd isp RemoveUser“ verwendet die folgende Syntax:

```
RemoveUser
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port .. .	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_se conds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_name	Erforderlich. Benutzerkonto, das Sie entfernen möchten.



# RemoveUserFromGroup

Entfernt einen nativen oder LDAP-Benutzer aus der nativen Gruppe in der Domäne.

Der Befehl „infacmd isp RemoveUserFromGroup“ verwendet die folgende Syntax:

```
RemoveUserFromGroup
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_name
[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
<-GroupName|-gn> group_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveUserFromGroup“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_name	Erforderlich. Name des Benutzers, den Sie entfernen möchten.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, den Sie entfernen möchten. Standardwert ist „Native“.
-GroupName -gn	group_name	Erforderlich. Name der Gruppe, aus der Sie den Benutzer entfernen möchten.

## RemoveUserPermission

Entfernt eine Benutzerberechtigung für ein Objekt.

Der Befehl „infacmd isp RemoveUserPermission“ verwendet die folgende Syntax:

```
RemoveUserPermission
<-DomainName|-dn> domain_name
```

```

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_name

[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]

<-ObjectName|-on> object_name

<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE

```

Die folgende Tabelle beschreibt die Optionen und Argumente für „infacmd isp RemoveUserPermission“:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert.
-ExistingUserName -eu	existing_user_name	Erforderlich. Name des Benutzers, dem Sie eine Berechtigung für ein Objekt zuweisen möchten.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, dem Sie eine Berechtigung zuweisen möchten. Standardwert ist „Native“.
-ObjectName -on	object_name	Name des Objekts, dem Sie die Benutzerzugriffsberechtigung entziehen möchten.
-ObjectType -ot	object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE	<p>Erforderlich. Typ des Objekts</p> <p>Geben Sie einen der folgenden Werte ein:</p> <ul style="list-style-type: none"> <li>- Dienst</li> <li>- License</li> <li>- Knoten</li> <li>- Gitter</li> <li>- Folder</li> <li>- OSProfile</li> </ul>

# RemoveUserPrivilege

Entfernt eine Berechtigung von einem Benutzer in der Domäne oder von einem Benutzer im Anwendungsdienst innerhalb der Domäne.

Der Befehl „infacmd isp RemoveUserPrivilege“ verwendet die folgende Syntax:

```
RemoveUserPrivilege
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_Name
[<-ExistingUserSecurityDomain|-esd> existing_user_security]
<-ServiceName|-sn> service_name
<-PrivilegePath|-pp> path_of_privilege
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveUserPrivilege“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	<p>Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.</p>
ExistingUserName -eu	existing_user_name	<p>Erforderlich. Benutzerkonto, aus dem Sie die Berechtigung entfernen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.</p>
-ExistingUserSecurityDomain -esd	existing_user_security_domain	<p>Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, dessen Berechtigung entfernt werden soll. Standardwert ist „Native“.</p>

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, für die bzw. den Sie Berechtigungen anzeigen möchten.
-PrivilegePath -pp	path_of_privilege	<p>Erforderlich. Vollqualifizierter Name der Berechtigung, die Sie der Gruppe zuweisen möchten. Ein vollqualifizierter Name enthält den Namen der Berechtigungsgruppe und den Namen der Berechtigung. Ein vollqualifizierter Berechtigungsname für den Repository-Dienst ist z. B. „folder/create“.</p> <p>Wenn der Berechtigungsname Leerzeichen enthält, setzen Sie den Pfad wie folgt in Anführungszeichen:</p> <pre>"Runtime Objects/Monitor/Execute/Manage Execution"</pre> <p>Wenn der Berechtigungsname das Sonderzeichen „/“ enthält, fügen Sie das Escape-Zeichen „\“ davor folgendermaßen ein:</p> <pre>"Model/View Model/Export\ /Import Models"</pre>

## RenameConnection

Benennt eine Verbindung um. Wenn Sie eine Verbindung umbenennen, aktualisieren das Developer-Tool und das Analyst-Tool die Jobs, die die Verbindung verwenden.

**Hinweis:** Bereitgestellte Anwendungen und Parameterdateien identifizieren eine Verbindung nach Namen, nicht nach Verbindungs-ID. Beim Umbenennen einer Verbindung müssen Sie daher alle Anwendungen erneut bereitstellen, die die Verbindung verwenden. Außerdem müssen Sie alle Parameterdateien aktualisieren, die den Verbindungsparameter verwenden.

Der Befehl „infacmd isp RenameConnection“ verwendet folgende Syntax:

```
RenameConnection
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConnectionName|-cn> connection_name
<-NewConnectionName|-ncn> new_connection_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RenameConnection“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.



Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ConnectionName -cn	connection_name	Erforderlich. Vorhandener Verbindungsname.
-NewConnectionName -ncn	new_connection_name	Erforderlich. Name der neuen Verbindung. Der Name unterliegt der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die maximale Länge beträgt 128 Zeichen. Das Leer- und die folgenden Sonderzeichen sind möglich: ~ ` ! \$ % ^ & * ( ) - + = { [ ] }   \ : ; " ' < , > . ? /

## ResetPassword

Setzt das Passwort für einen Benutzer in der Domäne zurück.

Der Befehl „infacmd isp ResetPassword“ verwendet die folgende Syntax:

```
ResetPassword
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ResetUserName|-ru> reset_user_name
<-ResetUserPassword|-rp> reset_user_password
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ResetPassword“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ResetUserName -ru	reset_user_name	Erforderlich. Name des Benutzers, dessen Passwort Sie zurücksetzen möchten.
-ResetUserPassword -rp	reset_user_password	<p>Erforderlich. Neues Passwort für den Benutzer. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -rp festgelegte Passwort Vorrang.</p> <p>Wenn Sie für ein natives Benutzerkonto die Passwortkomplexität aktivieren, beachten Sie beim Erstellen oder Ändern eines Passworts Folgendes:</p> <ul style="list-style-type: none"> <li>- Das Passwort muss aus mindestens acht Zeichen bestehen.</li> <li>- Es muss mindestens einen Buchstaben, eine Zahl und ein nicht alphanumerisches Zeichen enthalten, z. B.:</li> </ul> <pre>! \ " # \$ % &amp; ' ( ) * + , - . / : ; &lt; = &gt; ? @ [ ] ^ _ ` {   } ~</pre> <p>Manche Sonderzeichen in Passwörtern können von der Shell anders interpretiert werden. Beispielsweise wird \$ als Variable interpretiert. Setzen Sie in diesem Fall ein Escape-Zeichen vor das betreffende Sonderzeichen.</p>

## RunCPUProfile

Berechnet das CPU-Profil für einen Knoten.

**Hinweis:** Die Ausführung dieses Befehls dauert etwa fünf Minuten und lastet die CPU des Computers zu 100% aus.

Der Befehl „infacmd isp RunCPUProfile“ verwendet die folgende Syntax:

```
RunCPUProfile
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RunCPUProfile“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, für den Sie das CPU-Profil berechnen möchten.

# SetConnectionPermissions

Weist einem Benutzer oder einer Gruppe Verbindungsberechtigungen nach dem Entfernen der vorherigen Berechtigungen zu.

Der Befehl „`infacmd isp SetConnectionPermissions`“ verwendet die folgende Syntax:

```
SetConnectionPermissions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<<-RecipientUserName|-run> recipient_user_name|<RecipientGroupName|-rgn>
recipient_group_name>

<-RecipientSecurityDomain|-rsd> recipient_security_domain]

<-ConnectionName|-cn> connection_name

[<-Permission|-p> permission_READ|WRITE|EXECUTE|GRANT|ALL
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd isp SetConnectionPermissions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	Password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RecipientUserName -run	recipient_user_name	Erforderlich, wenn Sie den Gruppennamen des Empfängers nicht angeben. Name des Benutzers, dem Berechtigungen für die Verbindung zugewiesen werden
-RecipientGroupName -rgn	recipient_group_name	Erforderlich, wenn Sie den Benutzernamen des Empfängers nicht angeben. Name der Gruppe, der Berechtigungen für die Verbindung zugewiesen werden.
-RecipientSecurityDomain -rsd	recipient_security_domain_name	Erforderlich, wenn der Empfänger zu einer LDAP-Sicherheitsdomäne gehört. Name der Sicherheitsdomäne, zu der der Empfänger gehört. Standardwert ist „Native“.

Option	Argument	Beschreibung
-ConnectionName -cn	connection_name_security _domain	Erforderlich. Name der Verbindung.
-Permission -p	permission	Erforderlich. Typ der zuzuweisenden Berechtigung. Geben Sie mindestens einen der folgenden Werte durch Leerzeichen getrennt ein: <ul style="list-style-type: none"> <li>- READ</li> <li>- WRITE. Lesen und Schreiben.</li> <li>- EXECUTE</li> <li>- GRANT. Lesen und Gewähren.</li> <li>- ALL. Lesen, Schreiben, Ausführen, Gewähren</li> </ul>

## SetRepositoryLDAPConfiguration

Aktualisiert die LDAP-Serverkonfigurationsoptionen für ein PowerCenter-Repository.

Möglicherweise ist es erforderlich, die Verbindungsinformationen zwischen dem Repository und dem externen LDAP-Verzeichnisdienst nach der Installation von Informatica zu aktualisieren.

Verwenden Sie `infacmd isp ListRepositoryLDAPConfiguration`, um die aktuellen Werte für die LDAP-Serverkonfigurationsoptionen anzuzeigen.

Der Befehl „`infacmd isp SetRepositoryLDAPConfiguration`“ verwendet die folgende Syntax:

```
SetRepositoryLDAPConfiguration
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LDAPAddress|-la> ldap_server_address
<-SearchBase|-sb> search base
<-SearchScope|-ss> search scope
<-LDAPPrincipal|-lp> ldap_principal
<-LDAPCredential|-lc> ldap_credential
<-LoginAttribute|-lt> login attribute
<-LoginFilter|-lf> login filter
[<-UseSSL|-us> use_ssl]
[<-CertificateDatabase|-cd> certificate database for ssl]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp SetRepositoryLDAPConfiguration“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.



Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LDAPAddress -la	ldap_server_address	Erforderlich. Hostname und Portnummer für den Computer, auf dem der LDAP-Verzeichnisdienst gehostet wird. In der Regel weist der LDAP-Server die Portnummer 389 auf.
-SearchBase -sb	search base	Erforderlich. Distinguished Name (DN) des Eintrags, der als Ausgangspunkt für die Suche nach Benutzernamen in der LDAP-Verzeichnisstruktur verwendet wird. LDAP findet ein Objekt im Verzeichnis entsprechend dem Pfad im Distinguished Name des Objekts. Beispiel: In Microsoft Active Directory könnte der Distinguished Name des Benutzers cn=UserName,ou=OrganizationalUnit,dc=DomainName lauten, wobei die Reihe der durch dc=DomainName benannten relativen Distinguished Names die DNS-Domäne des Objekts kennzeichnet.
-SearchScope -ss	Suchbereich	Erforderlich. Bereich der Benutzersuche. Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none"> <li>- Basis. Durchsuchen Sie den durch die Suchbasis gekennzeichneten Eintrag.</li> <li>- Eine Ebene. Durchsuchen Sie alle Einträge eine Ebene unterhalb des Suchbasiseintrags, jedoch ausschließlich des Suchbasiseintrags.</li> <li>- Unterstruktur. Durchsuchen Sie die gesamte Unterstruktur auf allen Ebenen unterhalb des Suchbasiseintrags.</li> </ul>
-LDAPPrincipal -lp	ldap_principal	Erforderlich. Distinguished Name (DN) für den Prinzipal-Benutzer. Der Benutzername besteht häufig aus einem allgemeinen Namen (Common Name, CN), einer Organisation (Organization, O) und einem Land (Country, C). Der Name des Prinzipal-Benutzers bezeichnet einen Administratorbenutzer mit Zugriff auf das Verzeichnis und ist nicht der zu authentifizierende Name. Geben Sie einen Benutzer an, der über die Berechtigung zum Lesen anderer Benutzereinträge auf dem LDAP-Server verfügt. Lassen Sie diese Option aus, um sich als anonymer Benutzer anzumelden. Weitere Informationen erhalten Sie in der LDAP-Serverdokumentation.
-LDAPCredential -lc	ldap_credential	Erforderlich. Passwort für den Prinzipal-Benutzer. Sie können ein Passwort mit der Option -lc oder der Umgebungsvariable INFA_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -lc festgelegte Passwort Vorrang.  Lassen Sie diese Option aus, um sich als anonymer Benutzer anzumelden.
-LoginAttribute -lt	login_attribute	Erforderlich. Verzeichnisattribut, das Anmeldenamen enthält.

Option	Argument	Beschreibung
-LoginFilter -lf	login_filter	Erforderlich. Eine LDAP-Abfragezeichenfolge zum Filtern von Benutzersuchergebnissen. Der Filter kann Attributtypen, Assertionswerte und Vergleichskriterien angeben. Beispiel: (objectclass=*) durchsucht alle Objekte. (&(objectClass=user)(!(cn=susan))) sucht alle Benutzerobjekte außer „susan“. Weitere Informationen zu Suchfiltern erhalten Sie in der LDAP-Serverdokumentation.
-UseSSL -us	use_ssl	Verwenden Sie diese Option nicht. Informatica unterstützt keinen LDAP-Server, der SSL für 8.1.1-Versionen verwendet.
-CertificateDatabase -cd	certificate_database_for_ssl	Verwenden Sie diese Option nicht. Informatica unterstützt keinen LDAP-Server, der SSL für 8.1.1-Versionen verwendet.

## ShowLicense

Zeigt Lizenzdetails an. Die angezeigten Lizenzdetails sind ein kumulatives Ergebnis aller angewendeter Lizenzschlüssel. Der Dienstmanager aktualisiert die vorhandenen Lizenzdetails, wenn Sie einen inkrementellen Schlüssel zur Lizenz hinzufügen.

Um den `infacmd isp ShowLicense`-Befehl auszuführen, müssen Sie über Berechtigungen für die Lizenz verfügen.

Der Befehl „`infacmd isp ShowLicense`“ verwendet die folgende Syntax:

```
ShowLicense
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LicenseName|-ln> license_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ShowLicense“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz.

# ShutdownNode

Führt den Knoten herunter. Nach dem Starten des Knotens können Sie den Knoten neu starten, indem Sie den Informatica-Dienst auf dem Computer starten. Ein Knoten kann unter Verwendung von infacmd gestartet werden.

Der Befehl „infacmd isp ShutdownNode“ verwendet die folgende Syntax:

```
ShutdownNode

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ShutdownNode“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, den Sie herunterfahren möchten.

## SwitchToGatewayNode

Konvertiert einen vorhandenen Arbeitsknoten in einen Gateway-Knoten. Die Dienstrolle muss für den Arbeitsknoten aktiviert sein.

Der Befehl „infacmd isp SwitchToGatewayNode“ verwendet die folgende Syntax:

```
SwitchToGatewayNode
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
[<-EnableSaml|-saml> true|false]
[<-SamlTrustStoreDir|-std> saml_truststore_directory]
[<-SamlTrustStorePassword|-stp> saml_truststore_password]
[<-SamlKeyStoreDir|-skd> saml_keystore_directory]
[<-SamlKeyStorePassword|-skp> saml_keystore_password]
[<-AdminconsolePort|-ap> admin_tool_port]
[<-AdminconsoleShutdownPort|-asp> admin_tool_shutdown_port]
<-LogServiceDirectory|-ld> log_service_directory
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp SwitchToGatewayNode“ beschrieben:

Option	Beschreibung
-DomainName -dn	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	Erforderlich. Name des Knotens, den Sie in einen Gateway-Knoten umwandeln möchten.
-EnableSaml -saml	Optional. Aktiviert oder deaktiviert die SAML-Authentifizierung in der Informatica-Domäne.  Legen Sie diesen Wert auf „true“ fest, um die SAML-Authentifizierung in der Informatica-Domäne zu aktivieren. Der Standardwert ist „false“.

Option	Beschreibung
-SamlTrustStoreDir -std	Optional. Das Verzeichnis mit der benutzerdefinierten Truststore-Datei, die für die Verwendung der SAML-Authentifizierung auf dem Gateway-Knoten erforderlich ist. Geben Sie nur das Verzeichnis an, nicht den vollständigen Pfad zur Datei. Der Informatica-Standard-Truststore wird verwendet, wenn kein Truststore angegeben ist.
-SamlTrustStorePassword -stp	Erforderlich, wenn Sie einen benutzerdefinierten Truststore für die SAML-Authentifizierung verwenden. Das Passwort für den benutzerdefinierten Truststore.
-SamlKeyStoreDir -skd	Optional. Das Verzeichnis mit der benutzerdefinierten Truststore-Datei, die für die Verwendung der SAML-Authentifizierung auf dem Gateway-Knoten erforderlich ist. Geben Sie nur das Verzeichnis an, nicht den vollständigen Pfad zur Datei.
-SamlKeyStorePassword -skp	Erforderlich, wenn Sie einen benutzerdefinierten Schlüsselspeicher für die SAML-Authentifizierung verwenden. Passwort für den SAML-Schlüsselspeicher. *
-AdminconsolePort -ap	Port für den Zugriff auf Informatica Administrator.
-AdminconsoleShutdownPort -asp	Portnummer, die das Herunterfahren für Informatica Administrator steuert.
-LogServiceDirectory -ld	Erforderlich. Freigegebener Verzeichnispfad, der vom Protokollmanager zum Speichern von Protokollereignisdateien verwendet wird. Stellen Sie sicher, dass der Wert für -ld nicht übereinstimmt oder den angegebenen Wert für -sld enthält.
-DatabaseTruststorePassword -dbtp	Optional. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank. Erforderlich, wenn Sie eine sichere Domänenrepository-Datenbank für die Domäne konfigurieren.
-DatabaseTruststoreLocation -dbtl	Pfad und Dateiname der Truststore-Datei für die sichere Datenbank Erforderlich, wenn Sie eine sichere Domänenrepository-Datenbank für die Domäne konfigurieren.
Hinweis: Wenn Sie derzeit Skripts ausführen, die diesen Befehl verwenden, um einen benutzerdefinierten Schlüsselspeicher für die SAML-Authentifizierung zu aktivieren, müssen Sie diese aktualisieren, um diese Option aufzunehmen.	

## SwitchToWorkerNode

Wandelt einen Gateway-Knoten in einen Arbeitsknoten um. Der Befehl schlägt fehl, wenn der zu wechselnde Knoten der einzige Gateway-Knoten in der Domäne ist.

Wenn der Knoten als Master-Gateway-Knoten dient, müssen Sie ihn herunterfahren, bevor Sie ihn in einen Arbeitsknoten umwandeln können. Fahren Sie den Knoten herunter und warten Sie darauf, dass das Master-Gateway zur Ausfallsicherung an einen anderen Knoten übergeben wird. Sie können den Knoten dann neu starten und den infacmd isp SwitchToWorkerNode-Befehl ausführen.

Der Befehl „infacmd isp SwitchToWorkerNode“ verwendet die folgende Syntax:

```
SwitchToWorkerNode

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp SwitchToWorkerNode“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domännennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domännennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.



Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, den Sie in einen Arbeitsknoten umwandeln möchten.

## SyncSecurityDomains

Synchronisiert Benutzer und Gruppen in einer Sicherheitsdomäne mit den Benutzern und Gruppen im LDAP-Verzeichnisdienst.

Der Befehl „infacmd isp SyncSecurityDomains“ verwendet die folgende Syntax:

```
SyncSecurityDomains
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SynchronizingNamespace|-sn> namespace_to_sync
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp SyncSecurityDomain“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-SynchronizingNamespace -sn	namespace_to_sync	Name der Sicherheitsdomäne, die Sie mit dem LDAP-Verzeichnisdienst synchronisieren möchten.
-WaitCompletion -wc	true false	Optional. Gibt an, ob infacmd wartet, bis der Befehl abgeschlossen ist, bevor gemeldet wird, ob die Synchronisierung korrekt durchgeführt wurde oder fehlgeschlagen ist.  Mit „true“ wird gemeldet, wenn der Befehl nicht gestartet wird. Wenn der Befehl erfolgreich gestartet wird, wird gemeldet, ob die Synchronisierung korrekt durchgeführt wurde oder fehlgeschlagen ist.  Mit „false“ wird gemeldet, ob der Befehl gestartet wurde oder nicht, ohne den Abschluss der Synchronisierung abzuwarten.  Standardwert ist „false“.

## UnassignDefaultOSProfile

Entfernt das Betriebssystemprofil, das einem Benutzer oder einer Gruppe zugewiesen ist.

Der Befehl „infacmd isp UnassignDefaultOSProfile“ verwendet die folgende Syntax:

```
UnassignDefaultOSProfile
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-RecipientName|-nm> recipient_name
<-RecipientSecurityDomain|-ns> security_domain_of_recipient
<-RecipientType|-ty> recipient_type
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UnassignDefaultOSProfile“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-RecipientName -nm	recipient_name	Erforderlich. Benutzer- oder Gruppenname, der dem Standardbetriebssystemprofil zugewiesen wird.
-RecipientSecurityDomain -ns	security_domain_of_recipient	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, zu der der Benutzer gehört.
-RecipientType -ty	recipient_type	Erforderlich. Geben Sie an, ob das Standardbetriebssystemprofil einem Benutzer oder einer Gruppe zugewiesen werden soll. Geben Sie einen der folgenden Werte ein: - UserIdentity - GroupIdentity

## UnassignISMMService

Hebt die Verbindung zwischen dem PowerCenter-Integrationsdienst und dem Metadata Manager-Dienst auf. Wenn Sie einen PowerCenter-Integrationsdienst entfernen, müssen Sie einen anderen PowerCenter-Integrationsdienst verbinden, bevor Sie Ressourcen laden.

Der Befehl „infacmd isp UnassignISMMService“ verwendet die folgende Syntax:

```
UnassignISMMService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
```

```

<-Password|-pd> password

[<-SecurityDomain|-sdn> securitydomain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-IntegrationService|-is> integration_service_name

```

Die folgende Tabelle beschreibt die Optionen und Argumente für „infacmd isp UnassignISMMService“:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Metadata Manager-Diensts, dessen Zuweisung zum Integrationsdienst aufgehoben werden soll.
-IntegrationService -is	integration_service_name	Erforderlich. Name des Integrationsdiensts, dessen Zuordnung zum Metadata Manager-Dienst Sie aufheben möchten.

## UnassignLicense

Entfernt eine Lizenz aus einem Anwendungsdienst. Der Dienst muss gestoppt werden. Nachdem Sie eine Lizenz aus dem Dienst entfernt haben, müssen Sie eine gültige Lizenz zuweisen, um den Dienst erneut zu aktivieren.

Der Befehl „UnassignLicense“ verwendet die folgende Syntax:

```
UnassignLicense
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LicenseName|-ln> license_name
<-ServiceNames|-sn> service1_name service2_name ...
```

In der folgenden Tabelle werden die Optionen und Argumente für „*infacmd isp UnassignLicense*“ beschrieben:

Option	Argumente	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der <i>infacmd</i> versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet <i>infacmd</i> den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argumente	Beschreibung
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz, deren Zuweisung Sie aufheben möchten.
-ServiceNames -sn	service_name1 service_name2 ...	Erforderlich. Namen der Dienste, für die Sie die Lizenz entfernen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

## UnassignRoleFromGroup

Entfernt eine Rolle aus einer Gruppe für eine Domäne oder einen Anwendungsdienst.

Der Befehl „infacmd isp UnassignRoleFromGroup“ verwendet die folgende Syntax:

```
UnassignRoleFromGroup
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GroupName|-gn> group_name
[<-GroupSecurityDomain|-gsf> group_security_domain]
<-RoleName|-rn> role_name
<-ServiceName|-sn> service_name
```



In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UnassignRoleFromGroup“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GroupName -gn	group_name	Erforderlich. Name der Gruppe, aus der Sie eine Rolle entfernen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-GroupSecurityDomain -gsf	group_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der die Gruppe gehört, aus der Sie die Rolle entfernen. Standardwert ist „Native“.
-RoleName -rn	role_name	Erforderlich. Name der Rolle, die Sie aus der Gruppe entfernen möchten.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, aus der bzw. dem Sie die Rolle entfernen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

## UnassignRoleFromUser

Entfernt eine Rolle von einem Benutzer für eine Domäne oder einen Anwendungsdienst.

Der Befehl „infacmd isp UnassignRoleFromUser“ verwendet die folgende Syntax:

```
UnassignRoleFromUser
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_Name
[<-ExistingUserSecurityDomain|-esd> existing_user_securit
<-RoleName|-rn> role_name
<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UnassignRoleFromUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_Name	Erforderlich. Benutzerkonto, aus dem Sie die Rolle entfernen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, dessen Rolle entfernt werden soll. Standardwert ist „Native“.
-RoleName -rn	role_name	Erforderlich. Name der Rolle, die Sie für einen Benutzer entfernen möchten.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, aus der bzw. dem Sie die Rolle entfernen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

## UnassignRSWSHubService

Hebt die Verbindung zwischen einem PowerCenter-Repository und einem Web Services Hub in der Domäne auf.

Der Befehl „infacmd isp UnassignRSWSHubService“ verwendet die folgende Syntax:

```
UnassignRSWSHubService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-NodeName|-nn> node_name
<-RepositoryService|-rs> repository_service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UnassignRSWSHubService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Webdienst-Hubs, von dem Sie ein Repository trennen möchten.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Prozess des Webdienst-Hubs ausgeführt wird. Wenn die Informatica-Umgebung für hohe Verfügbarkeit konfiguriert ist, gibt diese Option den Namen des primären Knotens an.
-RepositoryService -rs	repository_service_name	Erforderlich. Name des Repository-Diensts, von dem der Webdienst-Hub abhängig ist.  Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

## UnassociateDomainNode

Trennen Sie den Knoten in einer Domäne von seiner Adresse. Der Knotenname bleibt Teil der Domäne, aber er hat keine physische Adresse.

In einer Domäne ist z. B. „Node1“ mit dem Computer „MyHost:9090“ verbunden. Wenn Sie diesen Befehl ausführen, wird die Verbindung zwischen dem Namen „Node1“ und der Hostadresse „MyHost:9090“ entfernt. Sie können „Node1“ dann mit einem neuen Host verbinden. Sie müssen den Befehl „infasetup DefineGatewayNode“ oder „DefineWorkerNode“ auf dem neuen Host ausführen, um „Node1“ auf diesem Computer zu definieren.

Der Befehl „infacmd isp UnassociateDomainNode“ verwendet die folgende Syntax:

```
UnassociateDomainNode
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UnassociateDomainNode“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, den Sie von der Domäne trennen möchten.

## UpdateConnection

Updates a connection. To list connection options, run infacmd isp ListConnectionOptions.

The infacmd isp UpdateConnection command uses the following syntax:

```
UpdateConnection
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConnectionName|-cn> connection_name
[<-ConnectionUserName|-cun> connection_user_name]
[<-ConnectionPassword|-cpd> connection_password]
[-o options] (name-value pairs separated by space)
```



The following table describes infacmd isp UpdateConnection options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	<p>Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.</p> <p>Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.</p>
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	<p>Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.</p> <p>If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConnectionName -cn	connection_name_security_domain	Required. Name of the connection to update.

Option	Argument	Description
ConnectionUserName -cun	connection_user_name	Required. Database user name.

Option	Argument	Description
-ConnectionPassword -cpd	connection_password	<p>Required. Password for the database user name. If you are updating an ADABAS, DB2I, DB2Z, IMS, SEQ, or VSAM connection, you can enter a valid PowerExchange passphrase instead of a password. Passphrases for access to databases and data sets on z/OS can be from 9 to 128 characters in length. Passphrases for access to DB2 for i5/OS can be up to 31 characters in length. Passphrases can contain the following characters:</p> <ul style="list-style-type: none"> <li>- Uppercase and lowercase letters</li> <li>- The numbers 0 to 9</li> <li>- Spaces</li> <li>- The following special characters: ' - ; # \ , . / ! % &amp; * ( ) _ + { } : @   &lt; &gt; ?</li> </ul> <p><b>Hinweis:</b> The first character is an apostrophe.</p> <p>Passphrases cannot include single quotation marks ('), double quotation marks ("), or currency symbols.</p> <p>If a passphrase contains spaces, you must enclose it with double-quotation marks ("), for example, "This is an example passphrase". If a passphrase contains special characters, you must enclose it with triple double-quotation characters ("""), for example, """"This passphrase contains special characters ! % &amp; * . """" . If a passphrase contains only alphanumeric characters without spaces, you can enter it without delimiters.</p> <p><b>Hinweis:</b> On z/OS, a valid RACF passphrase can be up to 100 characters in length. PowerExchange truncates passphrases longer than 100 characters when passing them to RACF for validation.</p> <p>To use passphrases, ensure that the PowerExchange Listener runs with a security setting of SECURITY=(1,N) or higher in the DBMOVER member. For more information, see "SECURITY Statement" in the <i>PowerExchange Reference Manual</i>.</p> <p>To use passphrases for IMS connections, ensure that the following additional requirements are met:</p> <ul style="list-style-type: none"> <li>- You must configure ODBA access to IMS as described in the <i>PowerExchange Navigator User Guide</i>.</li> <li>- You must use IMS data maps that specify IMS ODBA as the access method. Do not use data maps that specify the DL/1 BATCH access method because this access method requires the use of netport jobs, which do not support passphrases.</li> </ul>

Option	Argument	Description
		- The IMS database must be online in the IMS control region to use ODBA access to IMS.
- Options -o	options	Enter name-value pairs separated by spaces. To view valid options, run infacmd isp ListConnectionOptions.

## updateCustomLDAPType

Aktualisiert einen benutzerdefinierten LDAP-Typ, der einen LDAP-Verzeichnisdienst definiert, aus dem Sie Benutzer in eine LDAP-Sicherheitsdomäne importieren.

Der Befehl „infacmd isp updateCustomLDAPType“ verwendet die folgende Syntax:

```
updateCustomLDAPType
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-CustomLDAPTypeName|-lt> custom_LDAP_type_name
[<-DisplayName|-dpn> display_name]
[<-Uid> uid]
[<-GroupMembershipAttr|-gm> group_membership_attr]
[<-GroupDescriptionAttr|-gd> group_description_attr]
[<-UserSurnameAttr|-usn> user_surname_attr]
[<-UserGivenNameAttr|-ugn> user_given_name_attr]
[<-UserEmailAttr|-ue> user_email_attr]
[<-UserEnableAttr|-uen> user_enable_attr]
[<-UserTelephoneAttr|-utn> user_telephone_attr]
[<-UserDescriptionAttr|-ud> user_description_attr]
[<-CN> cn]
[<-FetchRangedAttr|-fr> fetch_ranged_attr]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp updateCustomLDAPType“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
- -CustomLDAPTypeName -lt	Name des benutzerdefinierten LDAP-Typs	Erforderlich. Der Name des zu aktualisierenden benutzerdefinierten LDAP-Typs.
- -DisplayName -dpn	Anzeigename	Optional. Name des benutzerdefinierten LDAP-Typs, der im Administrator Tool angezeigt wird.
-Uid	uid	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das den eindeutigen Bezeichner (UID) enthält, den der Dienstmanager zum Identifizieren von Benutzern verwendet.
- -GroupMembershipAttr -gm	Attribut „Gruppenmitgliedschaft“	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das Informationen zur Gruppenmitgliedschaft eines Benutzers enthält.
-GroupDescriptionAttr -gd	Attribut „Gruppenbeschreibung“	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das beschreibenden Text über die Gruppen im Verzeichnisdienst enthält.
-UserSurnameAttr -usn	Attribut „Nachname des Benutzers“	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das den Nachnamen eines Benutzers enthält.
-UserGivenNameAttr -ugn	Attribut „Vorname des Benutzers“	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das den Vornamen eines Benutzers enthält.
-GroupMembershipAttr -gm	LDAP_Group_Membership_Attribute	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das die Namen der Gruppen im Verzeichnisdienst enthält.
--UserEmailAttr -ue	Attribut „E-Mail des Benutzers“	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das die E-Mail-Adresse eines Benutzers enthält.
-UserEnableAttr -uen	Attribut „Benutzeraktivierung“	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das enthält
- UserTelephoneAttr -utn	Attribut „Telefonnummer des Benutzers“	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das die Telefonnummer eines Benutzers enthält.
- User DescriptionAttr -ud	Attribut „Benutzerbeschreibung“	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das eine Beschreibung des Benutzers enthält.

Option	Argument	Beschreibung
-CN	cn	Optional. Name des Attributs im LDAP-Verzeichnisdienst, das das Attribut mit dem vollständigen Namen oder dem gebräuchlichen Namen eines Benutzers enthält.
- FetchRangedAttr -fr	Attribut „Bereich abrufen“	Optional. Auf true festlegen, um alle Werte abzurufen, die in Attributen mit mehreren Werten enthalten sind. Verwenden Sie diese Option nur für Microsoft Active Directory.

## UpdateDomainOptions

Aktualisiert Domäneneigenschaften. Die Domäneneigenschaften beinhalten Resistenz-Timeout, Grenzwert für Resistenz-Timouts, maximale Neustartversuche, Neustartzeitraum, TLS-Modus und Sendemodus.

Der Befehl „infacmd isp UpdateDomainOptions“ verwendet die folgende Syntax:

```
UpdateDomainOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-DomainOptions|-do> option_name=value ...
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateDomainOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.



Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-DomainOptions -do	option_name=value	<p>Erforderlich. Domäneneigenschaften, die Sie aktualisieren möchten. Sie können die folgenden Eigenschaften aktualisieren:</p> <ul style="list-style-type: none"> <li>- LicenseUsageDetailMinDays. Die Mindestanzahl an Tagen, an denen der Protokollmanager Protokollereignisse für die Lizenznutzung aufbewahrt.</li> <li>- LicenseUsageSummaryMinDays. Die Mindestanzahl an Tagen, an denen der Protokollmanager Datensätze für die Lizenznutzung aufbewahrt.</li> <li>- ResilTimeout. Zeitraum in Sekunden, in dem Dienste versuchen, als Clients eine Verbindung zu anderen Diensten herzustellen.</li> <li>- RestartsMaxAttempts. Anzahl der in einem angegebenen Zeitraum durchgeführten Versuche der Domäne, einen Anwendungsdienstprozess neu zu starten, wenn dieser fehlschlägt.</li> <li>- RestartsWithinSeconds. Maximaler Zeitraum in Sekunden, in dem die Domäne versucht, einen Anwendungsdienstprozess neu zu starten, wenn dieser fehlschlägt.</li> <li>- ServiceResilTimeout. Maximaler Zeitraum, in dem der Dienst Ressourcen beibehält, um Resistenz-Timeouts zu entsprechen.</li> <li>- TaskDispatchMode. Load Balancer-Sendemodus für Aufgaben: RoundRobin, MetricBased oder Adaptive. Starten Sie den Integrationsdienst neu, damit die Änderungen wirksam werden.</li> <li>- TLSMode. Konfiguriert die sichere Kommunikation zwischen Diensten innerhalb der Domäne. Starten Sie die Domäne neu, damit die Änderungen wirksam werden. Gültige Werte sind „true“ oder „false“.</li> </ul>

## UpdateFolder

Aktualisiert die Ordnerbeschreibung.

Der Befehl „infacmd isp UpdateFolder“ verwendet die folgende Syntax:

```
UpdateFolder
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
```

```
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
<-FolderPath|-fp> full_folder_path
```

```
<-FolderDescription|-fd> description_of_folder
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateFolder“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-FolderPath -fp	full_folder_path	Erforderlich. Vollständiger Pfad (ohne Domänenname) des Ordners, den Sie aktualisieren möchten. Folgendes Format ist erforderlich:  <i>/parent_folder/child_folder</i>
-FolderDescription -fd	description_of_folder	Erforderlich. Beschreibung des Ordners. Wenn die Ordnerbeschreibung Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen.

## UpdateGatewayInfo

Aktualisiert die Konnektivitätsinformationen für den Gateway-Knoten in der domains.infa-Datei.

Führen Sie „infacmd isp UpdateGatewayInfo“ zum Erstellen oder Aktualisieren einer domains.infa-Datei aus. Die Datei „domains.infa“ enthält die Verbindungsdaten für einen Gateway-Knoten in einer Domäne sowie die TLS- und Kerberos-Konfiguration der Domäne. Zu den Konnektivitätsinformationen gehören der Domänenname sowie Name und HTTP-Port des Domänenhosts.

Unter Umständen müssen Sie eine domains.infa-Datei erzeugen, um infacmd oie-Befehle auf einem Client-Computer auszuführen. Führen Sie zum Erzeugen der Datei „domains.infa“ den Befehl „infacmd isp UpdateGatewayInfo“ aus. Der Befehl „updateGatewayInfo“ erzeugt eine domains.infa-Datei im DeveloperClient-Verzeichnis. Definieren Sie den Hostnamen und Port des Domänen-Gateways, wenn Sie den Befehl ausführen.

Der infacmd isp UpdateGatewayInfo-Befehl verwendet die folgende Syntax:

```
UpdateGatewayInfo
<-DomainName|-dn> domain_name
<-GatewayAddress|-dg> domain_gateway_host:port
[<-Force|-f>]
```

In der folgenden Tabelle werden infacmd isp UpdateGatewayInfo-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-GatewayAddress -dg	domain_gateway_host:port	Erforderlich. Name und Portnummer des Gateway-Hostcomputers. Geben Sie die Gateway-Adresse im folgenden Format ein:  domain_gateway_host:port
-Force -f	-	Optional. Aktualisiert oder erstellt die Datei „domains.infa“ auch dann, wenn die Verbindung zur Domäne fehlschlägt. Die Option -Force legt die Kerberos- und TLS-fähigen Optionen in der Datei „domains.infa“ als „false“ fest, wenn die Verbindung zur Domäne fehlschlägt. Wenn Sie die Option -Force nicht angeben, aktualisiert der Befehl die Datei „domains.infa“ nicht, wenn die Verbindung zur Domäne fehlschlägt.

## UpdateGrid

Aktualisiert die Liste der Knoten, die einem Gitter zugewiesen sind.

Der Befehl „infacmd isp UpdateGrid“ verwendet die folgende Syntax:

```
UpdateGrid
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GridName|-gn> grid_name
<-NodeList|-nl> node1 node2 ...
[<-UpdateNodeList|-ul> true|false]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateGrid“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GridName -gn	grid_name	Erforderlich. Name des Gitters.

Option	Argument	Beschreibung
-NodeList -nl	node1 node2 ...	Erforderlich. Namen der Knoten, die Sie dem Gitter zuweisen möchten. Diese Knotenliste ersetzt oder aktualisiert die Liste der zuvor dem Gitter zugewiesenen Knoten auf Basis der definierten Option -ul.  Wenn Sie die Option -ul angeben, aktualisiert die Option -nl die Liste der zuvor dem Gitter zugewiesenen Knoten. Wenn Sie die Option -ul nicht angeben, ersetzt die Option -nl die Liste der zuvor dem Gitter zugewiesenen Knoten.
-UpdateNodeList -ul	true false	Optional. Aktualisiert die aktuelle Knotenliste mit den Werten in der Option -nl, anstatt die Liste der zuvor dem Gitter zugewiesenen Knoten zu ersetzen. Wenn TRUE, aktualisiert infacmd die Knotenliste mit der Liste der Knoten, die mithilfe der Option -nl angegeben wurden, sowie mit den zuvor dem Gitter zugewiesenen Knoten. Wenn FALSE, ersetzt infacmd die Knotenliste mit der Liste der Knoten, die mithilfe der Option -nl angegeben wurden. Standardwert ist „False“.

## UpdateIntegrationService

Aktualisiert die Konfigurationseigenschaften für den PowerCenter-Integrationsdienst.

Der Befehl „infacmd isp UpdateIntegrationService“ verwendet die folgende Syntax:

```
UpdateIntegrationService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
[<-NodeName|-nn> node_name<-GridName|-gn> grid_name]
[<-BackupNodes|-bn> node1 node2 ...]
[<-RepositoryService|-rs> repository_service_name]
[<-RepositoryUser|-ru> repository_user]
[<-RepositoryPassword|-rp> repository_password]
[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]
[<-ServiceOptions|-so> option_name=value ...]
```

**Hinweis:** Für infacmd isp UpdateIntegrationService dürfen die Optionen -ru, -rp und -rsdn nicht in der Kerberos-Authentifizierung verwendet werden. Wenn Sie diese Optionen im Kerberos-Modus verwenden, schlägt der Befehl fehl.

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateIntegrationService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Integrationsdiensts. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Integrationsdienstprozess ausgeführt wird. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, gibt diese Option den Namen des primären Knotens an. Geben Sie keinen Wert für diese Option ein, wenn Sie den Gitternamen angeben.
-GridName -gn	grid_name	Optional. Name des Gitters, in dem der Integrationsdienstprozess ausgeführt wird. Geben Sie keinen Wert für diese Option ein, wenn Sie den Knotennamen angeben.
-BackupNodes -bn	node1 node2 ...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Sicherungsknoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.
-RepositoryService -rs	repository_service_name	Optional. Name des Repository-Diensts, von dem der Integrationsdienst abhängig ist. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryUser -ru	user	Erforderlich für native und LDAP-Authentifizierung. Benutzername zum Herstellen einer Verbindung zum Repository. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryPassword -rp	Passwort	Erforderlich für native und LDAP-Authentifizierung. Benutzerpasswort. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -rp festgelegte Passwort Vorrang.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Erforderlich für LDAP-Authentifizierung. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der PowerCenter-Repository-Benutzer gehört. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung. Wenn Sie diese Option nicht angeben, setzt der Befehl die Sicherheitsdomäne des Repository-Benutzers auf nativ.
-ServiceOptions -so	option_name=value	Optional. Dienstigenschaften, mit denen definiert wird, wie der PowerCenter-Integrationsdienst ausgeführt wird.



# updateLDAPConnectivity

Aktualisiert die angegebene LDAP-Konfiguration.

Der Befehl „`infacmd isp updateLDAPConnectivity`“ verwendet die folgende Syntax:

```
updateLDAPConnectivity
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LDAPAddress|-la> ldap_server_address
[<-LDAPPrincipal|-lp> ldap_principal]
[<-LDAPCredential|-lc> ldap_credential]
[<-UseSSL|-us> use_ssl]
[<-TrustLDAPCertificate|-tc> trust_ldap_certificate]
<-LDAPType|-lt> ldap_types=MicrosoftActiveDirectory, MicrosoftAzureActiveDirectory,
SunJavaSystemDirectory, NovellE-Directory, IBMTivoliDirectory, OpenLDAP,
OracleDirectoryServerODSEE, OracleUnifiedDirectory, <Custom LDAP Type Name>
[<-MaxSecurityDomainSize|-ms> Max_Security_Domain_size]
[<-GroupMembershipAttr|-gm> LDAP_Group_Membership_Attribute]
[<-LDAPNotCaseSensitive|-lnc> ldap_not_case_sensitive]
<-LDAPHostConfigurationName|-lcn> LDAP_host_configuration_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp updateLDAPConnectivity“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LDAPAddress -la	ldap_server_address	Erforderlich. Hostname und Portnummer für den Computer, auf dem der LDAP-Verzeichnisdienst gehostet wird. In der Regel weist der LDAP-Server die Portnummer 389 auf. Wenn der LDAP-Server SSL verwendet, lautet dessen Portnummer 636.
-LDAPPrincipal -lp	ldap_principal	Optional. Distinguished Name (DN) für den Prinzipal-Benutzer. Lassen Sie diese Option aus, um sich als anonymer Benutzer anzumelden.  Weitere Informationen finden Sie in der Dokumentation für den LDAP-Verzeichnisdienst.
-LDAPCredential -lc	ldap_credential	Optional. Passwort für den Prinzipal-Benutzer. Sie können ein Passwort mit der Option -lc oder der Umgebungsvariablen INFA_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -lc festgelegte Passwort Vorrang.  Lassen Sie diese Option aus, um sich als anonymer Benutzer anzumelden.
-UseSSL -us	use_ssl	Optional. Wenn Sie die Option einbeziehen, verwendet der LDAP-Verzeichnisdienst das SSL-Protokoll (Secure Socket Layer).
-TrustLDAPCertificate -tc	trust_ldap_certificate	Optional. Wenn Sie die Option einbeziehen, stellt PowerCenter eine Verbindung zum LDAP-Server ohne Überprüfung des SSL-Zertifikats aus.  Wenn Sie die Option nicht einbeziehen, stellt PowerCenter vor dem Herstellen einer Verbindung zum LDAP-Server sicher, dass das SSL-Zertifikat von einer Zertifizierungsstelle signiert ist.
-LDAPType -lt	ldap_types=value	Erforderlich. Typ des LDAP-Verzeichnisdiensts. Verzeichnisdienste umfassen: <ul style="list-style-type: none"> <li>- MicrosoftActiveDirectory</li> <li>- Microsoft Azure Active Directory</li> <li>- SunJavaSystemDirectory</li> <li>- NovellE-Directory</li> <li>- IBMTivoliDirectory</li> <li>- OpenLDAP</li> <li>- Oracle Directory Server (ODSEE)</li> <li>- Oracle Unified Directory</li> </ul> Wenn Sie einen benutzerdefinierten LDAP-Verzeichnisdienst verwenden, geben Sie den Namen des Diensts an.

Option	Argument	Beschreibung
-MaxSecurityDomainSize -ms	Max_Security_Domain_size	Optional. Maximale Anzahl an Benutzerkonten zum Importieren in eine Sicherheitsdomäne. Standardwert ist „1000“.
-GroupMembershipAttr -gm	LDAP_Group_Membership_Attribute	Optional. Name des Attributs, das Informationen zur Gruppenmitgliedschaft eines Benutzers enthält.
-LDAPNotCaseSensitive -lnc	LDAP_Not_Case_Sensitive	Optional. Gibt an, dass die Benutzernamen aus dem LDAP-Verzeichnisdienst der Groß-/Kleinschreibung nicht unterliegen. Standardwert ist „false“.
-LDAPHostConfigurationName -lcn	LDAP-Hostkonfigurationsname	Erforderlich. Der Name der zu aktualisierenden LDAP-Konfiguration.

## UpdateLicense

Aktualisiert die Lizenzinformationen für die Domäne. Führen Sie diesen Befehl aus, um Ihre Lizenz mit einem inkrementellen Lizenzschlüssel zu aktualisieren. Sie verwenden diesen Schlüssel, um lizenzierte Optionen hinzuzufügen oder zu entfernen.

Wenn Sie einer Lizenz einen inkrementellen Schlüssel hinzufügen, aktualisiert der Dienstmanager das Lizenzablaufdatum, wenn das Ablaufdatum für den inkrementellen Schlüssel nach dem des ursprünglichen Schlüssels liegt.

Der Befehl „infacmd isp UpdateLicense“ verwendet die folgende Syntax:

```
UpdateLicense
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LicenseName|-ln> license_name
<-LicenseKeyFile|-lf> license_key_file
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateLicense“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-LicenseName -ln	license_name	Erforderlich. Name des Lizenzobjekts, das Sie aktualisieren möchten.
-LicenseKeyFile -lf	license_key_file	Erforderlich. Name und Pfad der Datei, die den inkrementellen Schlüssel enthält.

## UpdateMMService

Aktualisiert oder erstellt die Dienstoptionen für einen Metadata Manager-Dienst. Um die Dienstoptionen zu aktualisieren oder zu erstellen, deaktivieren Sie den Metadata Manager-Dienst, aktualisieren Sie die Optionen und aktivieren Sie den Dienst erneut.

Der Befehl „infacmd isp UpdateMMService“ verwendet die folgende Syntax:

```
UpdateMMService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
[<-LicenseName|-ln> license_name]
<-ServiceOptions|-so> option_name=value ...>
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateMMService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Metadata Manager-Diensts, den Sie aktualisieren möchten.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz, die Sie dem Metadata Manager-Dienst zuweisen möchten.
-ServiceOptions -so	option_name=value	Optional. Diensteigenschaften, mit denen definiert wird, wie der Metadata Manager-Dienst ausgeführt wird.

## UpdateMonitoringOptions

Aktualisiert die allgemeinen Eigenschaften, um Aktionen in der Domäne zu überwachen.

Wenn Sie einen Modellrepository-Dienst mit der Option -ModelRepositoryService festlegen, müssen Sie auch Werte für die Optionen -RepositoryUserName und -RepositoryPassword eingeben. Sie müssen Werte für alle drei oder für keine der Optionen angeben.

Der Befehl `infacmd isp UpdateMonitoringOptions` verwendet die folgende Syntax:

```
UpdateMonitoringOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-ModelRepositoryService|-rs> model_repository_service]
[<-RepositoryUserName|-rsun> model_repository_user_name]
[<-RepositoryPassword|-rspd> model_repository_password]
[<-RepositorySecurityDomain|-rsdn> model_repository_security_domain]
[<-AdministratorOptions|-ao> option_name=value ... (MaxSortedRecords, ShowMilliseconds)]
[<-CachingOption|-co> option_name=value ... (DefaultNotificationDelay)]
[<-PurgeOptions|-po> option_name=value ... (PurgeScheduleTime, PurgeTaskFrequency,
StatisticsExpiryTime, DetailedStatisticsExpiryTime)]
```



In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateMonitoringOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Anzahl der Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang. Standardwert ist 180 Sekunden.
-ModelRepositoryService -rs	model_repository_service	Optional. Name des Modellrepository-Diensts, der die Verlaufsdaten speichert.
-RepositoryUserName -rsun	model_repository_user_name	Erforderlich für native und LDAP-Authentifizierung. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Benutzername zum Zugriff auf den Modellrepository-Dienst.
-RepositoryPassword -rspd	model_repository_password	Erforderlich für native und LDAP-Authentifizierung. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Benutzerpasswort zum Zugriff auf den Modellrepository-Dienst.
-RepositorySecurityDomain -rsdn	model_repository_security_domain	Erforderlich für LDAP- oder Kerberos-Authentifizierung. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Benutzer des PowerCenter-Repositorys gehört. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Wenn Sie diese Option nicht angeben, setzt der Befehl die Sicherheitsdomäne des Repository-Benutzers auf nativ.
-AdministratorOptions -ao	option_name=value	Optional. Allgemeine Verwaltungseinstellungen für Datensätze und Überwachungsberichte. Sie können die folgenden Optionen einrichten: <ul style="list-style-type: none"> <li>- MaxSortedRecords. Maximale Anzahl der Datensätze, die sortiert werden können. Standardwert ist 3.000.</li> <li>- ShowMilliseconds. Einschließlich Millisekunden für Datums- und Uhrzeitfeld in Überwachungsberichten. Kann auf „True“ oder „False“ eingestellt werden. Standardwert ist „False“.</li> </ul>

Option	Argument	Beschreibung
-CachingOption -co	option_name=value	Optional. Einstellungen für das Zwischenspeichern von Statistiken. Sie können die folgenden Optionen einrichten: <ul style="list-style-type: none"> <li>- DefaultNotificationDelay. Maximale Anzahl der Sekunden, die der Datenintegrationsdienst die Statistiken puffert, bevor er die Statistiken im Modellrepository beibehält und sie in einen Überwachungsbericht schreibt. Standardwert ist 10.</li> </ul>
-PurgeOptions -po	option_name=value	Optional. Einstellungen für das Bereinigen von Statistiken. Sie können die folgenden Optionen einrichten: <ul style="list-style-type: none"> <li>- PurgeScheduleTime. Uhrzeit, zu der der Modellrepository-Dienst Statistiken bereinigt. Standardwert ist 1:00 morgens.</li> <li>- PurgeTaskFrequency. Intervall in Tagen, in dem der Modellrepository-Dienst Statistiken bereinigt, die älter als die für die ExpiryTime-Optionen konfigurierten Werte sind. Standardwert ist 1.</li> <li>- StatisticsExpiryTime. Anzahl an Tagen, die das Modellrepository gemittelte Statistiken speichert. Wenn die Bereinigung deaktiviert ist, werden die Statistiken unbegrenzt im Modellrepository gespeichert. Standardwert ist 180. Minimalwert ist 0. Maximalwert ist 366.</li> <li>- DetailedStatisticsExpiryTime. Anzahl an Tagen, die das Modellrepository minutengenaue Statistiken speichert. Wenn die Bereinigung deaktiviert ist, werden die Statistiken unbegrenzt im Modellrepository gespeichert. Standardwert ist 14. Minimalwert ist 1. Maximalwert ist 14.</li> </ul>

## UpdateNamespace

Aktualisiert eine LDAP-Sicherheitsdomäne mit den Filtern für den Benutzer und die Gruppe. Aktualisiert die LDAP-Sicherheitsdomäne, wenn die Informatica-Domäne LDAP oder die Kerberos-Authentifizierung verwendet.

Der Befehl „infacmd isp UpdateNamespace“ verwendet die folgende Syntax:

```
UpdateNamespace
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```

<-NameSpace|-ns> namespace

[<-UserSearchBase|-usb> usersearchbase]

[<-UserFilter|-uf> userfilter]

[<-GroupSearchBase|-gsb> groupsearchbase]

[<-GroupFilter|-gf> groupfilter]

[<-LDAPHostConfigurationName|-lcn> LDAP_host_configuration_name]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateNamespace“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Sie können einen Wert für -sdn angeben oder den Standardwert basierend auf dem Authentifizierungsmodus verwenden:</p> <ul style="list-style-type: none"> <li>- Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Standardwert ist „Nativ“. Zum Arbeiten mit der LDAP-Authentifizierung müssen Sie den Wert für -sdn angeben.</li> <li>- Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Standardwert ist „Native“ für native Authentifizierung. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</li> </ul>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn Sie die Umgebungsvariable nicht angeben, wird der Standardwert von 180 Sekunden verwendet.
-NameSpace -ns	namespace	<p>Erforderlich. Name der LDAP- oder Kerberos-Sicherheitsdomäne. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf weder Leerzeichen noch folgende Sonderzeichen enthalten:</p> <p>, + / &lt; &gt; @ ; \ % ?</p> <p>Der Name darf nicht länger als 128 Zeichen sein. Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Sie können keine anderen Leerzeichen verwenden.</p>
-UserSearchBase -usb	usersearchbasesu	<p>Distinguished Name (DN) des Eintrags, der als Ausgangspunkt für die Suche nach Benutzernamen im LDAP-Verzeichnisdienst dient. Der LDAP-Verzeichnisdienst sucht nach einem Objekt im Verzeichnis entsprechend dem Pfad im Distinguished Name des Objekts.</p> <p>Beispiel: In Microsoft Active Directory könnte der Distinguished Name des Benutzers cn=UserName,ou=OrganizationalUnit,dc=DomainName lauten. Die Reihe der durch dc=DomainName benannten relativen Distinguished Names kennzeichnet die DNS-Domäne des Objekts.</p>

Option	Argument	Beschreibung
-UserFilter -uf	userfilter	Ein LDAP-Abfragestring, der die Suchkriterien für die Suche nach Benutzern im Verzeichnisdienst festlegt. Der Filter kann Attributtypen, Assertionwerte und Abgleichkriterien angeben.  Beispiel: Der Filter (objectclass=*) sucht alle Objekte. Der Filter (&(objectClass=user) (!(cn=susan))) sucht alle Benutzerobjekte außer „susan“. Weitere Informationen über Suchfilter finden Sie in der Dokumentation für den LDAP-Verzeichnisdienst:
-GroupSearchBase -gsb	groupsearchbase	Distinguished Name (DN) des Eintrags, der als Ausgangspunkt für die Suche nach Gruppennamen im LDAP-Verzeichnisdienst dient.
-GroupFilter -gf	groupfilter	Ein LDAP-Abfragestring, der die Kriterien für die Suche nach Gruppen im Verzeichnisdienst festlegt.
-LDAPHostConfigurationName -lcn	ldapName	Optional. Der Name der LDAP-Konfiguration, die der Sicherheitsdomäne zugeordnet ist.

## UpdateNodeOptions

Aktualisiert allgemeine Knoteneigenschaften, wie z. B. das Backup-Verzeichnis, das CPU-Profil, die Fehlerschweregradstufe, Dienstprozessports und Ressourcenbereitstellungsgrenzen.

Der Befehl „infacmd isp UpdateNodeOptions“ verwendet die folgende Syntax:

```
UpdateNodeOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
[<-NodeOptions|-no> option_name=value ...]
[<-ResourceProvision|-rp> option_name=value ...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateNodeOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-NodeName -nn	node_name	Optional. Name des Knotens, dessen Ressourcenbereitstellungsgrenzen aktualisiert werden sollen.
-NodeOptions -no	option_name=value	<p>Optional. Die Knotenoptionen, die Sie aktualisieren möchten. Sie können die folgenden Optionen aktualisieren:</p> <ul style="list-style-type: none"> <li>- BackupDir. Verzeichnis zum Speichern der Repository-Backup-Dateien.</li> <li>- CPUProfile. Einstufung der CPU-Leistung des Knotens im Vergleich zum Baseline-System. ErrorSeverityLevel. Level der Fehlerprotokollierung für den Knoten: error, warning, info, trace, debug.</li> <li>- MaxProcessPort. Höchste von den Dienstprozessen auf dem Knoten verwendete Portnummer.</li> <li>- MinProcessPort. Niedrigste von den Dienstprozessen auf dem Knoten verwendete Portnummer.</li> </ul> <p>Das folgende Beispiel legt MaxProcessPort auf 1515 fest:</p> <pre>infacmd UpdateNodeOptions ... -no MaxProcessPort=1515</pre>
-ResourceProvision -rp	option_name=value	<p>Optional. Die Ressourcenbereitstellungsgrenzen, die Sie aktualisieren möchten. Sie können die folgenden Schwellenwerte aktualisieren:</p> <ul style="list-style-type: none"> <li>- MaxCPURunQueueLength. Die maximale Anzahl an ausführbaren Threads, die auf CPU-Ressourcen auf dem Knoten warten.</li> <li>- MaxMemoryPercent. Der maximale Prozentsatz des virtuellen Speichers, der auf dem Knoten relativ zur Gesamtgröße des physischen Speichers zugeordnet ist.</li> <li>- MaxProcesses. Die maximale Anzahl an Sitzungs- und Befehlsaufgaben, die in jedem auf dem Knoten ausgeführten Integrationsdienst ausgeführt werden können.</li> </ul> <p>Das folgende Beispiel legt MaxProcesses auf 15 fest:</p> <pre>infacmd UpdateNodeOptions ... -rp MaxProcesses=15</pre>

## UpdateNodeRole

Aktualisiert die Rolle auf einem Knoten in der Domäne. Sie können die Dienst- oder Berechnungsrolle auf einem Knoten aktivieren oder deaktivieren.

Standardmäßig verfügt jeder Knoten sowohl über die Dienstrolle als auch die Berechnungsrolle. Wenn ein Knoten einem Datenintegrationsdienst-Gitter zugewiesen wird, können Sie die Knotenrolle bei Bedarf aktualisieren. Aktivieren Sie nur die Dienstrolle, wenn der Knoten den Datenintegrationsdienst-Prozess ausführen soll. Aktivieren Sie nur die Berechnungsrolle, wenn der Knoten Datenintegrationsdienst-Mappings ausführen soll.

Wenn Sie die Rolle auf einem Knoten aktualisieren, der einem Datenintegrationsdienst oder einem Datenintegrationsdienstgitter zugewiesen ist, müssen Sie den Datenintegrationsdienst recyceln, damit die Änderungen wirksam werden.



Der `infacmd isp UpdateNodeRole`-Befehl verwendet die folgende Syntax:

```
UpdateNodeRole

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

[<-EnableServiceRole|-esr> true|false]

[<-EnableComputeRole|-ecr> true|false]

[<-disableComputeRoleMode|-mo> disable_mode]
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd isp UpdateNodeRole`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des zu aktualisierenden Knotens.
-EnableServiceRole -esr	true   false	<p>Optional. Aktiviert die Dienstrolle auf dem Knoten. Bei „True“ können Anwendungsdienste auf dem Knoten ausgeführt werden. Bei „False“ können Anwendungsdienste nicht auf dem Knoten ausgeführt werden. Legen Sie den Befehl nur auf „False“ fest, wenn der Knoten einem Datenintegrationsdienst-Gitter zugewiesen ist und Sie den Knoten für ausgeführte Mappings dedizieren möchten.</p> <p>Standardwert ist „True“.</p>

Option	Argument	Beschreibung
-EnableComputeRole -esr	true   false	Optional. Aktiviert die Berechnungsrolle auf dem Knoten. Bei „True“ kann der Knoten Berechnungen durchführen, die von Remote-Anwendungsdiensten angefragt werden. Bei „False“ kann der Knoten keine von Remote-Anwendungsdiensten angefragten Berechnungen durchführen. Für einen Knoten ist die Berechnungsrolle erforderlich, wenn der Datenintegrationsdienst Jobs auf diesem Knoten ausführt. Wenn der Datenintegrationsdienst auf diesem Knoten keine Jobs ausführt, können Sie die Berechnungsrolle deaktivieren. Eine aktivierte oder deaktivierte Berechnungsrolle hat allerdings keine Auswirkungen auf die Leistung. Standardwert ist „True“.
-disableComputeRoleMode -mo	disable_mode	Optional. Legt fest, wie die Berechnungsrolle deaktiviert wird: <ul style="list-style-type: none"> <li>- Abschließen. Berechnungen können abgeschlossen werden, bevor die Berechnungsrolle deaktiviert wird.</li> <li>- Stoppen. Stoppt alle laufenden Berechnungen und deaktiviert dann die Berechnungsrolle.</li> <li>- Abbrechen. Versucht, alle laufenden Berechnungen vor deren Abbruch und der Deaktivierung der Berechnungsrolle zu stoppen.</li> </ul> Standardwert ist „Abbrechen“.

## UpdateOSProfile

Aktualisiert Eigenschaften für ein Betriebssystemprofil in der Domäne.

**Hinweis:** Um Arbeitsabläufe auszuführen, die Betriebssystemprofile verwenden, benötigen Sie die Betriebssystemprofil-Option.

Der Befehl „infacmd isp UpdateOSProfile“ verwendet die folgende Syntax:

```
UpdateOSProfile
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-OSProfileName|-on> OSProfile_name
[<-IntegrationServiceProcessOptions|-po> option_name=value ...]
[<-DISProcessVariables|-diso> option_name=value ...]
[<-DISEnvironmentVariables|-dise> name=value ...]
[<-HadoopImpersonationProperties|-hipr> hadoop_impersonation_properties]
[<-HadoopImpersonationUser|-hu> hadoop_impersonation_user]
```

```
[<-UseLoggedInUserAsProxy|-ip> use_logged_in_user_as_proxy]
```

```
[<-ProductExtensionName|-pe> product_extension_name]
```

```
[<-ProductOptions|-o> optionGroupName.optionName=Value ...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateOSProfile“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port .. .	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-OSProfileName -on	OSProfile_name	Erforderlich. Name des Betriebssystemprofils.
-IntegrationServiceProcessOptions -po	option_name=value	Optional. Dienstprozesseigenschaften, mit denen definiert wird, wie der PowerCenter-Integrationsdienst ausgeführt wird.
-EnvironmentVariables -ev	name=value	Optional. Name und Wert von Umgebungsvariablen, die vom PowerCenter-Integrationsdienst zur Laufzeit verwendet werden.
-DISProcessVariables -diso	option_name=value	Optional. Dienstprozesseigenschaften, mit denen definiert wird, wie der Datenintegrationsdienst ausgeführt wird.
-DISEnvironmentVariables -dise	name=value	Optional. Name und Wert von Umgebungsvariablen, die vom Datenintegrationsdienst zur Laufzeit verwendet werden.

Option	Argument	Beschreibung
-HadoopImpersonationProperties -hipr	hadoop_impersonation_properties	Optional. Gibt an, ob der Datenintegrationsdienst den Hadoop-Identitätswechselbenutzer zum Ausführen von Mappings, Arbeitsabläufen und Profiling-Aufträgen in einer Hadoop-Umgebung verwendet. Gültige Werte sind „True“ oder „False“.
-HadoopImpersonationUser -hu	hadoop_impersonation_user	Optional. Geben Sie einen Benutzernamen für den Datenintegrationsdienst zum Identitätswechsel an, wenn er einen Auftrag in einer Hadoop-Umgebung ausführt.
-UseLoggedInUserAsProxy -ip	use_logged_in_user_as_proxy	Optional. Gibt an, ob der angemeldete Benutzer als Hadoop-Identitätswechselbenutzer verwendet werden soll. Gültige Werte sind „True“ oder „False“.
-ProductExtensionName -pe	product_extension_name	Optional. Für zukünftige Verwendung reserviert.
-ProductOptions -o	optionGroupName.optionName=Value	<p>Erforderlich. Name und Wert jeder von Ihnen festgelegten Option. Erstellen Sie mit dieser Option ein Cache-Verzeichnis für Einfachdateien, das vom Betriebssystemprofil verwendet werden kann.</p> <p>Mit dem folgenden Befehl wird das Cache-Verzeichnis beispielsweise auf „\$PMRootDir/OSPCache“ festgelegt:</p> <pre>infacmd isp createOSProfile ... -o 'runTimeVariables.flatFileCacheDirectory'="\$PMRootDir/OSPCache"</pre>

## UpdateRepositoryService

Aktualisiert oder erstellt Dienstoptionen für den PowerCenter-Repository-Dienst.

Sie können z. B. den Betriebsmodus des PowerCenter-Repository-Diensts aktualisieren und auf „normal“ oder „exklusiv“ festlegen. Im normalen Modus können mehrere Benutzer auf den PowerCenter-Repository-Dienst zugreifen und Repository-Inhalte aktualisieren. Im exklusiven Modus kann ein einzelner Benutzer auf den PowerCenter-Repository-Dienst zugreifen und Repository-Inhalte aktualisieren. Legen Sie den Betriebsmodus auf exklusiv fest, wenn Sie Verwaltungsaufgaben durchführen, die erfordern, dass sich ein einzelner Benutzer anmeldet und die Konfiguration aktualisiert. Um den Betriebsmodus des PowerCenter-Repository-Diensts zu aktualisieren, deaktivieren Sie den PowerCenter-Repository-Dienst, aktualisieren Sie den Betriebsmodus und aktivieren Sie den PowerCenter-Repository-Dienst dann erneut.

Der Befehl „infacmd isp UpdateRepositoryService“ verwendet die folgende Syntax:

```
UpdateRepositoryService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
```

```

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

[<-NodeName|-nn> node_name]

[<-BackupNodes|-bn> node1 node2 ...]

[<-ServiceOptions|-so> option_name=value ...]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateRepositoryService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des zu aktualisierenden PowerCenter-Repository-Diensts. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der PowerCenter-Repository-Dienstprozess ausgeführt wird. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, gibt diese Option den Namen des primären Knotens an.
-BackupNodes -bn	node1 node2 ...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Sicherungsknoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.
-ServiceOptions -so	option_name=value	Erforderlich. Diensteigenschaften, mit denen definiert wird, wie der PowerCenter-Repository-Dienst ausgeführt wird.

## Repository-Dienst-Optionen (-so)

Geben Sie Repository-Dienst-Optionen im folgenden Format ein:

```
infacmd CreateRepositoryService ... -so option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Repository-Dienst-Optionen beschrieben:

Option	Beschreibung
AllowWritesWithRACaching	Optional. Verwendet PowerCenter Client-Tools zum Ändern von Metadaten im Repository, wenn „RepAgent cachén“ aktiviert ist. Standardwert ist „Ja“.
CheckinCommentsRequired	Optional. Beim Einchecken von Repository-Objekten müssen Benutzer Kommentare hinzufügen. Standardwert ist „Ja“. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
CodePage	Erforderlich. Codepage-Beschreibung für die Datenbank. Zur Eingabe einer Codepage, die ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.



Option	Beschreibung
ConnectionString	Erforderlich. Die während der Einrichtung des PowerCenter-Repository-Diensts angegebene Datenbankverbindungszeichenfolge. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
DBPassword	Erforderlich. Repository-Datenbankpasswort für den Datenbankbenutzer. Sie können ein Passwort mit der Option -so oder der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -so festgelegte Passwort Vorrang. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
DBPoolExpiryThreshold	Optional. Die Mindestanzahl an inaktiven Datenbankverbindungen, die im PowerCenter-Repository-Dienst zulässig sind. Beispiel: Wenn 20 inaktive Verbindungen vorhanden sind und Sie diesen Schwellenwert auf 5 festlegen, schließt der PowerCenter-Repository-Dienst höchstens 15 Verbindungen. Die Mindestanzahl beträgt 3. Standardwert ist 5.
DBPoolExpiryTimeout	Optional. Der Zeitraum in Sekunden, in dem der PowerCenter-Repository-Dienst nach inaktiven Datenbankverbindungen sucht. Ist eine Verbindung für einen Zeitraum inaktiv, der diesen Wert überschreitet, kann der PowerCenter-Repository-Dienst die Verbindung schließen. Der Mindestwert beträgt 300. Der Höchstwert beträgt 2.592.000 (30 Tage). Standardwert ist 3.600 (1 Stunde).
DBUser	Erforderlich. Konto für die Datenbank, die das Repository enthält. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
DatabaseArrayOperationSize	Optional. Anzahl der Zeilen, die bei jedem Array-Datenbankvorgang abgerufen werden, beispielsweise Einfügen oder Abrufen. Standardwert ist 100. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
DatabaseConnectionTimeout	Optional. Zeitraum in Sekunden, in dem der PowerCenter-Repository-Dienst versucht, eine Verbindung zum Datenbankverwaltungssystem herzustellen. Standardwert ist 180.
DatabasePoolSize	Optional. Maximale Anzahl der Verbindungen zur Repository-Datenbank, die der PowerCenter-Repository-Dienst herstellen kann. Der Mindestwert beträgt 20. Standardwert ist 500.
DatabaseType	Erforderlich. Typ der Datenbank, die die Repository-Metadaten speichert. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
EnableRepAgentCaching	Optional. Aktiviert die Funktion „Repository Agent Caching“. Standardwert ist „Ja“.
ErrorSeverityLevel	Optional. Mindestebene der Fehlermeldungen, die in das PowerCenter-Repository-Dienstprotokoll geschrieben werden: <ul style="list-style-type: none"> <li>- Fatal</li> <li>- Fehler</li> <li>  Warnung</li> <li>- Info</li> <li>- Trace</li> <li>- Debug</li> </ul> Der Standardwert lautet „Info“.

Option	Beschreibung
HeartBeatInterval	Optional. Zeitraum, in dem der PowerCenter-Repository-Dienst seine Verbindungen zu den Clients in diesem Dienst überprüft. Standardwert ist 60 Sekunden.
MaxResilienceTimeout	Optional. Maximaler Zeitraum in Sekunden, in dem der Dienst die Ressourcen zwecks Belastbarkeit beibehält. Standardwert ist 180.
MaximumConnections	Optional. Maximale Anzahl der Verbindungen, die das Repository von den Repository-Clients akzeptiert. Standardwert ist 200.
MaximumLocks	Optional. Maximale Anzahl an Sperren, die das Repository für Metadatenobjekte verwendet. Standardwert ist 50.000.
OperatingMode	Optional. Modus, in dem der PowerCenter-Repository-Dienst ausgeführt wird: <ul style="list-style-type: none"> <li>- Normal</li> <li>- Exklusiv</li> </ul> Standardwert ist „Normal“. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
OptimizeDatabaseSchema	Optional. Optimierte das Repository-Datenbankschema beim Erstellen von Repository-Inhalten oder Sichern und Wiederherstellen eines IBM DB2- oder Microsoft SQL Server-Repositorys. Bei Aktivierung versucht der PowerCenter-Repository-Dienst Repository-Tabellen zu erstellen, die Varchar-Spalten mit einer Genauigkeit von 2000 anstelle von CLOB-Spalten enthalten. Verwenden Sie Varchar-Spalten, um die Leistung des Repositorys zu steigern. Bei Verwendung von Varchar-Spalten verringern Sie die Festplatteneingabe und -ausgabe und die Datenbank kann die Spalten zwischenspeichern. Um diese Option zu verwenden, überprüfen Sie die Anforderungen an die Seitengröße für die folgenden Repository-Datenbanken: <ul style="list-style-type: none"> <li>- IBM DB2. Datenbank-Seitengröße 4 KB oder größer. Mindestens einen temporären Tablespace mit einer Seitengröße von mindestens 16 KB.</li> <li>- Microsoft SQL Server. Datenbank-Seitengröße 8 KB oder größer.</li> </ul> Standardwert ist „Deaktiviert“.
PreserveMXData	Optional. Behält MX-Daten für frühere Versionen von Zuordnungen bei. Standardwert ist „Deaktiviert“.
RACacheCapacity	Optional. Anzahl der Objekte, die der Cache bei aktiviertem Repository Agent Caching enthalten kann. Standardwert ist 10.000.
SecurityAuditTrail	Optional. Verfolgt Änderungen, die an Benutzern, Gruppen und Berechtigungen vorgenommen wurden. Standardwert ist „Nein“.
ServiceResilienceTimeout	Optional. Zeitraum in Sekunden, in dem der Dienst versucht, eine Verbindung zu einem anderen Dienst herzustellen oder erneut herzustellen. Standardwert ist 180. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
TableOwnerName	Optional. Name des Eigentümers der Repository-Tabellen für ein IBM DB2-Repository.
TablespaceName	Optional. Tablespace-Name für IBM DB2-Repositorys. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
TrustedConnection	Optional. Verwendet Windows-Authentifizierung, um auf die Microsoft SQL Server-Datenbank zuzugreifen. Standardwert ist „Nein“. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.

# UpdateSAPBWService

Aktualisiert den Dienst und die Dienstprozessoptionen für den SAP BW-Dienst.

Der Befehl „infacmd isp UpdateSAPBWService“ verwendet die folgende Syntax:

```
UpdateSAPBWService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

[<-NodeName|-nn> node_name]

[<-ServiceOptions|-so> option_name=value ...]

[<-ServiceProcessOptions|-po> option_name=value ...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateSAPBWService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Name des SAP BW-Diensts erforderlich. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der SAP BW-Dienstprozess ausgeführt wird. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, gibt diese Option den Namen des primären Knotens an.
-ServiceOptions -so	option_name=value	Optional. Diensteigenschaften, mit denen definiert wird, wie der SAP BW-Dienst ausgeführt wird.
-ServiceProcessOptions -po	option_name=value	Optional. Dienstprozesseigenschaften, mit denen definiert wird, wie der SAP BW-Dienstprozess ausgeführt wird.

# UpdateServiceLevel

Aktualisiert die Eigenschaften der Dienstebene. Sie können die Dispatch-Priorität und die maximale Dispatch-Wartezeit aktualisieren.

Der Befehl „infacmd isp UpdateServiceLevel“ verwendet die folgende Syntax:

```
UpdateServiceLevel  
  
<-DomainName|-dn> domain_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-SecurityDomain|-sdn> security_domain]  
  
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]  
  
<-ServiceLevelName|-ln> service_level_name  
  
<-ServiceLevel|-sl> option_name=value ...
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateServiceLevel“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceLevelName -ln	service_level_name	Erforderlich. Name der Dienstebene, die Sie aktualisieren möchten.
-ServiceLevel -sl	option_name=value	Erforderlich. Die Eigenschaften der Dienstebene, die Sie aktualisieren möchten. Sie können die folgenden Eigenschaften aktualisieren: <ul style="list-style-type: none"> <li>- DispatchPriority. Die anfängliche Priorität für den Versand. Kleinere Zahlen haben höhere Priorität. Priorität 1 ist die höchste Priorität.</li> <li>- MaxDispatchWaitTime. Der Zeitraum in Sekunden, bevor der Load Balancer die Dispatch-Priorität für eine Aufgabe in die höchste Priorität eskaliert.</li> </ul>

## UpdateServiceProcess

Aktiviert die Werte der PowerCenter-Integrationsdienst-Prozessoptionen.

Der Befehl „infacmd isp UpdateServiceProcess“ verwendet die folgende Syntax:

```
UpdateServiceProcess
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
```

```

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

<-ServiceProcessOptions|-po> option_name=value
[<-ProcessEnvironmentVariables|-ev> option_name=value ...]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateServiceProcess“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Diensts. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem Sie Konfigurationsinformationen aktualisieren möchten.
-ServiceProcessOptions -po	option_name=value	<p>Name und neue Werte der Optionen, deren Werte Sie aktualisieren möchten. Sie können mehrere option_name=value-Paare angeben. Sie können eine Prozessvariable im Wert verwenden.</p> <p>Zum Beispiel legt der folgende Befehl das Cache-Verzeichnis auf „\$PMRootDir/NewCache“ und das Verzeichnis der Ablehnungsdatei auf „\$PMRootDir/NewBadFiles“ fest.</p> <pre>infacmd UpdateServiceProcess ... -po \$PMCacheDir=\$PMRootDir/NewCache \$PMBadFileDir= \$PMRootDir/NewBadFiles</pre> <p>Erforderlich, wenn Sie ProcessEnvironmentVariables nicht angeben.</p>
-ProcessEnvironmentVariables -ev	option_name=value	<p>Umgebungsvariablen für den Dienstprozess. Sie können mehrere Umgebungsvariablen angeben.</p> <p>Zum Beispiel fügt der folgende Befehl das JAVA_HOME-Verzeichnis zu „\$HOME/java“ und das INFA_HOME-Verzeichnis zu „\$HOME/Informatica/9.0.1/install“ für den angegebenen Dienstprozess hinzu oder aktualisiert die Verzeichnisse entsprechend.</p> <pre>infacmd ProcessEnvironmentVariables ... -ev JAVA_HOME=\$HOME/java INFA_HOME=\$HOME/ Informatica/9.0.1/install</pre> <p>Erforderlich, wenn Sie ServiceProcessOptions nicht angeben.</p>



# UpdateSMTPOptions

Aktualisiert die SMTP-Konfiguration der Domäne. Die SMTP-Konfiguration dient zum Senden von Domänenwarnungen und Scorecard-Benachrichtigungen.

Nach dem Konfigurieren der SMTP-Einstellungen müssen Sie mit dem AddAlertUser-Befehl Alarme für den Benutzer abonnieren.

Der infacmd isp UpdateSMTPOptions-Befehl verwendet die folgende Syntax:

```
UpdateSMTPOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SMTPAddress|-sa> smtp_server_address

[<-SMTPUsername|-su> user_name]

[<-SMTPPassword|-sp> password]

[<-SMTPSenderAddress|-ss> sender_email_address]

[<-ResetSMTPUserNameAndPassword|-re> reset_smtp_username_password]

[<-TLSEnabled|-tls> is_tls_enabled]
```

In der folgenden Tabelle werden infacmd isp UpdateSMTPOptions-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	password	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Nativ“.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-SMTPAddress -sa	SMTP_server_address	Erforderlich. Der Hostname und die Portnummer für den ausgehenden SMTP-Mailserver. Geben Sie diese Informationen in folgendem Format ein: <i>host_name:port_number</i>
-SMTPUserName -su	user_name	Optional. Benutzername für die Authentifizierung beim Senden, wenn dies vom ausgehenden Mailserver gefordert wird.
-SMTPPassword -sp	password	Benutzerpasswort für die Authentifizierung beim Senden, wenn dies vom ausgehenden Mailserver gefordert wird. Sie können ein Passwort mit der Option -sp oder der Umgebungsvariable INFA_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -sp festgelegte Passwort Vorrang.
-SMTPSenderAddress -ss	sender_email_address	Optional. Die vom Dienstmanager zum Senden von Benachrichtigungs-E-Mails verwendete E-Mail-Adresse. Wenn Sie dieses Feld leer lassen, verwendet der Dienstmanager den Standardwert „Administrator@<host>“ als Senderadresse.
-ResetSMTPUserNameAndPassword -re	reset_smtp_username_password	Optional. Konfigurieren Sie die Einstellungen für den ausgehenden SMTP-Mailserver, damit ein Benutzer Alarme abonnieren kann.
-TLSEnabled -tls	is_tls_enabled	Optional. Gibt an, dass der SMTP-Server das TLS-Protokoll verwendet. Wenn TRUE, geben Sie die TLS-Portnummer für die Eigenschaft des SMTP-Serverports ein. Geben Sie TRUE oder FALSE ein. Standardwert ist „false“.

## VERWANDTE THEMEN:

- [“AddAlertUser” auf Seite 367](#)

# UpdateWSHubService

Aktualisiert einen Web Services Hub in der Domäne.

Der Befehl „infacmd isp UpdateWSHubService“ verwendet die folgende Syntax:

```
UpdateWSHubService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

[<-NodeName|-nn> node_name]

[<-ServiceOptions|-so> option_name=value ...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateWSHubService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Webdienst-Hubs, den Sie aktualisieren möchten.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Prozess des Webdienst-Hubs ausgeführt wird.
-ServiceOptions -so	option_name=value ...	Optional. Diensteigenschaften, mit denen definiert wird, wie der Webdienst-Hub ausgeführt wird.

# UpgradeGatewayNodeMetadata

Aktualisiert die Metadaten für einen Gateway-Knoten auf dem aktuellen Computer. Führen Sie vor dem Aktualisieren des Gateway-Knotens den Befehl „`infacmd isp ShutDownNode`“ aus, um den Knoten herunterzufahren.

Der Befehl „`UpgradeGatewayNodeMetadata`“ verwendet die folgende Syntax:

```
UpdateGatewayNode
[<-LogServiceDirectory|-ld> log_service_directory (used for GatewayNode only)]
[<-SystemLogDirectory|-sld> system_log_directory]
[<-HttpsPort|-hs> https_port]
[<-KeystoreFile|-kf> keystore_file_location]
[<-KeystorePass|-kp> keystore_password]
<<-DatabaseAddress|-da> database_hostname:database_port|<-DatabaseConnectionString|-cs>
database_connection_string>
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE|POSTGRESQL
[<-DatabaseServiceName|-ds> database_service_name]
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for MSSQLServer and PostgreSQL only)]
[<-TrustedConnection|-tc> trusted_connection (used for MSSQLServer only)]
<-PreviousInfaHome|-ph> previous_infa_home
[<-KeysDirectory|-kd> Infa_secrets_directory_location]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
```

In der folgenden Tabelle werden *infa*setup-Optionen und -Argumente für „`UpgradeGatewayNodeMetadata`“ beschrieben:

Option	Beschreibung
-LogServiceDirectory -ld	Erforderlich. Freigegebener Verzeichnispfad, der vom Protokollmanager zum Speichern von Protokollereignisdateien verwendet wird. Stellen Sie sicher, dass -ld nicht übereinstimmt oder den angegebenen Wert für -sld enthält.
-SystemLogDirectory -sld	Optional. Verzeichnispfad zum Speichern von Systemprotokolldateien. Stellen Sie sicher, dass -ld nicht übereinstimmt oder den angegebenen Wert für -sld enthält. Standardwert ist <INFA_home>/logs.
-HttpsPort -hs	Optional. Portnummer, die vom Knoten für die Kommunikation zwischen dem Administrator Tool und dem Dienstmanager verwendet wird. Geben Sie diese Portnummer an, wenn Sie HTTPS für einen Knoten konfigurieren möchten. Zum Deaktivieren von HTTPS-Unterstützung für einen Knoten setzen Sie diese Portnummer auf Null.
-KeystoreFile -kf	Optional. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die bei Verwendung des SSL-Protokolls erforderlich sind
-KeystorePass -kp	Optional. Ein Klartext-Passwort für die Schlüsselspeicherdatei. Sie können ein Passwort mit der Option -kp oder der Umgebungsvariable INFA_PASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -kp festgelegte Passwort Vorrang.
-DatabaseAddress -da	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Name und Portnummer des Computers, auf dem die Konfigurationsdatenbank der Domäne gehostet wird.

Option	Beschreibung
-DatabaseConnectionString -cs	Erforderlich, wenn Sie die Optionen -DatabaseAddress (-da) und -DatabaseServiceName (-ds) nicht verwenden. Verbindungszeichenfolge, die zum Herstellen einer Verbindung zur Konfigurationsdatenbank der Domäne verwendet wird. Geben Sie den Namen des Datenbankhosts, -ports und -diensts als Teil der Verbindungszeichenfolge ein. Setzen Sie die Verbindungszeichenfolge in Anführungszeichen.
-DatabaseUserName -du	Erforderlich, wenn Sie die Option -TrustedConnection (-tc) nicht verwenden. Konto für die Datenbank, die die Domänenkonfigurationsinformationen enthält.
-DatabasePassword -dp	Passwort aus der Datenbank für die Domänenkonfiguration des Datenbankbenutzers. Wenn Sie diese Option weglassen, verwendet <i>infasetup</i> das in der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD angegebene Passwort. Wird in der Umgebungsvariable kein Wert angegeben, müssen Sie ein Passwort unter Verwendung dieser Option eingeben.
-DatabaseType -dt	Erforderlich. Typ der Datenbank, in der die Domänenkonfigurationsmetadaten gespeichert werden. Zu den Datenbanktypen gehören: <ul style="list-style-type: none"> <li>- db2</li> <li>- oracle</li> <li>- mssqlserver</li> <li>- sybase</li> <li>- postgresql</li> </ul>
-DatabaseServiceName -ds	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Der Name des Datenbankdiensts. Erforderlich für Oracle-, IBM DB2- und Microsoft SQL Server-Datenbanken. Geben Sie die SID für Oracle, den Dienstnamen für IBM DB2 oder den Datenbanknamen für Microsoft SQL Server ein.
-Tablespace -ts	Erforderlich für eine IBM DB2-Datenbank. Name des Tablespace, in dem sich die Datenbanktabellen für die Domänenkonfiguration befinden.
-SchemaName -sc	Optional. Name des Microsoft SQL Server-Schemas. Geben Sie einen Schemanamen ein, wenn Sie nicht das Standardschema verwenden.
-TrustedConnection -tc	Optional. Stellen Sie eine Verbindung zur Microsoft SQL Server-Datenbank über eine vertrauenswürdige Verbindung her. Die vertrauenswürdige Authentifizierung verwendet die Windows-Sicherheitsanmeldedaten des aktuellen Benutzers, um eine Verbindung zu Microsoft SQL Server herzustellen.
-PreviousInfaHome -ph	Erforderlich. Pfad zum vorherigen Informatica-Startverzeichnis.
-KeysDirectory -kd	Optional. Verzeichnis, in dem alle Schlüsseltabellendateien und der Verschlüsselungsschlüssel für die Informatica-Domäne gespeichert werden. Standardwert ist <Informatica-Installationsverzeichnis>/isp/config/keys.
-DatabaseTlsEnabled -dbtls	Optional. Gibt an, ob die Informatica-Domänendatenbank mit TLS und SSL sicher ist. Setzen Sie diese Option für die sichere Datenbank auf True. Standardwert ist „False“. Wenn die Option -dbtls ohne Wert angegeben wird, verwendet die Informatica-Domäne die sichere Kommunikation mit der Informatica-Domänendatenbank.

Option	Beschreibung
-DatabaseTruststorePassword -dbtp	Optional. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.
-DatabaseTruststoreLocation -dbtl	Optional. Pfad und Dateiname der Truststore-Datei für den Gateway-Knoten.

## validateFeature

Validiert, dass die Funktion in der angegebenen Plug-In-Datei in der Domäne registriert ist.

Der Befehl „`infacmd isp validateFeature`“ verwendet die folgende Syntax:

```
validateFeature
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-FeatureFilename|-ff> feature_filename
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd isp validateFeature`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie den Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-FeatureFilename -ff	feature_filename	Erforderlich. Pfad und Dateiname der Plug-In-XML-Datei der registrierten Funktion, die Sie validieren möchten.

## Version

Zeigt die PowerCenter-Version, die Marke Informatica sowie Urheberrechtsinformationen an.

Der version-Befehl verwendet die folgende Syntax:

```
infacmd version
```



# KAPITEL 22

## infacmd Idm-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [backupContents, 821](#)
- [CreateService, 824](#)
- [ListServiceOptions, 830](#)
- [ListServiceProcessOptions, 832](#)
- [migrateContents, 833](#)
- [publishArchive, 837](#)
- [restoreContents, 839](#)
- [UpdateServiceOptions, 842](#)
- [UpdateServiceProcessOptions, 844](#)
- [upgrade, 846](#)

### backupContents

Der Katalogdienst erstellt ein Backup der MongoDB-, Solr-, PostgreSQL- und Scanner-Staging-Daten. Vor dem Sichern des Katalogdiensts müssen Sie die folgenden Umgebungsvariablen festlegen:

- **INFA\_TRUSTSTORE.** Mithilfe des folgenden Beispielbefehls können Sie die Variable festlegen: `export INFA_TRUSTSTORE= <Speicherort der Informatica-Truststore-Datei>`. Standardspeicherort ist `$INFA_HOME/services/shared/security`.
- **INFA\_KEYSTORE.** Mithilfe des folgenden Beispielbefehls können Sie die Variable festlegen: `export INFA_KEYSTORE=<Speicherort der Schlüsselspeicherdatei>`. Standardspeicherort ist `$INFA_HOME/services/shared/security`. Diese Variable ist nur erforderlich, wenn Sie eine Konfiguration mit benutzerdefinierter SSL für die Informatica-Domäne verwendet haben. Für Konfigurationen mit Standard-SSL und ohne SSL müssen Sie die Variable aufheben.
- **Verschlüsseltes INFA\_TRUSTSTORE\_PASSWORD.** Verschlüsseln Sie das von Ihnen festgelegte Passwort. Mithilfe des folgenden Beispielbefehls können Sie das verschlüsselte Passwort festlegen: `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA=="`.
- **Verschlüsseltes INFA\_KEYSTORE\_PASSWORD.** Verschlüsseln Sie das von Ihnen festgelegte Passwort. Mithilfe des folgenden Beispielbefehls können Sie das verschlüsselte Passwort festlegen: `export INFA_KEYSTORE_PASSWORD="6cDE/ItyUL/Rtui9nhVRI=="`. Diese Variable ist nur erforderlich, wenn Sie eine Konfiguration mit benutzerdefinierter SSL für die Informatica-Domäne verwendet haben. Für Konfigurationen mit Standard-SSL und ohne SSL müssen Sie die Variable aufheben.

**Hinweis:** Mithilfe des folgenden Beispielbefehls können Sie das verschlüsselte Passwort festlegen: \$INFA HOME/server/bin/pmpasswd <password>

Beispiel:

- export INFA\_KEYSTORE\_PASSWORD=hQDP8O8tfwxRSwbeANEptl4AIQqJcSj9ZMDkVK+9S+Y=
- export INFA\_TRUSTSTORE\_PASSWORD=hx/nRWisSjnQ0zEGV3N7j1FCGF0m5RfisQxKTdf5f8Y=
- export INFA\_TRUSTSTORE=/data/Informatica/LDM1051/services/shared/security/
- export INFA\_KEYSTORE=/data/Informatica/LDM1051/services/shared/security

Beachten Sie vor der Ausführung dieses Befehls die folgenden Punkte:

- Wenn der Katalogdienst aktiv ist und die Sicherung läuft, können Sie den Lesevorgang im Katalogdienst ausführen.
- Wenn Solr auf mehreren Knoten bereitgestellt wird, sollte das gemeinsam genutzte Dateipfadsystem des Clusters für alle Solr-Hosts identisch sein, das gemeinsam genutzte Clusterpfadsystem eine NFS-Bereitstellung sein und die Gateway-Benutzer-ID für alle Solr-Hosts identisch sein.
- Für den Befehl BackupContents sind die Umgebungsvariablen INFA\_KEYSTORE und INFA\_KEYSTORE\_PASSWORD erforderlich, um eine Verbindung zu den Solr- und MongoDB-Diensten des Informatica-Cluster-Diensts herzustellen.
- Legen Sie die Umgebungsvariablen INFA\_TRUSTSTORE und INFA\_TRUSTSTORE\_PASSWORD für die Informatica-Domäne sowohl mit als auch ohne SSL fest.
- Wenn Solr in einer Konfiguration mit mehreren Knoten installiert ist, müssen Sie die Option ClusterSharedFilesystemPath im Informatica-Cluster-Dienst zum Wiederherstellen von Solr verwenden.

Der Befehl „infacmd ldm BackupContents“ verwendet die folgende Syntax:

```
BackupContents
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-OutputFilename|-of> output_file_name
[<-Force|-fr> force
[<-StoreType|-st> Comma separated values of backup store type to be taken. Accepted
types are Asset,Orchestration,Search,Similarity. Example value:
'Asset,Search,Orchestration' or simply 'Search'). By default, it will take backup for
all stores.]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd Idm BackupContents“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Katalogdiensts.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-OutputFilename -of	output_file_name	Erforderlich. Vollständiger Pfad und Dateiname der ZIP-Sicherungsdatei auf dem lokalen Computer. Der Befehl „backup“ erstellt den Namen der ZIP-Datei.
-Force -fr	force	Optional. Wenn eine Sicherung erzwungen werden soll, während der Sicherungsmodus offline ist. Erzwingt die Sicherung und überschreibt die vorhandene Sicherung.
-StoreType -st	Werte des Datenspeichertyps: - Asset - Orchestration - Search - Similarity	<p>Optional. Geben Sie den erforderlichen Datenspeicher, den Sie sichern möchten, oder eine durch Kommas getrennte Liste der Datenspeicher an, die Sie sichern möchten.</p> <p>Basierend auf den Problemen, die Sie beheben möchten, können Sie die erforderlichen Datenspeicher sichern, anstatt eine vollständige Sicherung des Katalogs zu erstellen.</p> <p>Sie können die folgenden Datenspeicher im Katalog sichern:</p> <ul style="list-style-type: none"> <li>- Asset</li> <li>- Orchestration</li> <li>- Search</li> <li>- Similarity</li> </ul> <p>Sie müssen die Werte <b>Asset</b>, <b>Search</b> und <b>Similarity</b> sichern, wenn Sie Daten anzeigen möchten, nachdem Sie Daten aus der Sicherung wiederhergestellt haben.</p> <p><b>Hinweis:</b> Standardmäßig sichert der Befehl alle Datenspeicher im Katalog.</p> <p>Weitere Informationen finden Sie in den folgenden Beispielen:</p> <ul style="list-style-type: none"> <li>- Um Datenspeicher zu sichern, die „Asset“, „Similarity“, „Search“ und „Orchestration“ enthalten, fügen Sie die Option <b>-st</b> wie gezeigt hinzu: <code>-st Asset, Similarity, Search, Orchestration</code>.</li> </ul>

Ab Enterprise Data Catalog 10.5.1.1 können Sie den Status der Sicherung in der folgenden Protokolldatei auf dem Knoten anzeigen, auf dem Sie den Befehl ausführen: `<Informatica installation directory>/logs/<Node name>/services/CatalogService/<Catalog Service name>/LDMBackup.log`. Die maximale Dateigröße für jede Protokolldatei beträgt 100 MB. Nach Erreichen der maximalen Dateigröße wird eine neue Datei erstellt. Maximal 20 Protokolldateien können gespeichert werden. Nach Erreichen dieses Grenzwerts wird die älteste Protokolldatei durch die neueste Protokolldatei ersetzt.

## CreateService

Erstellt einen Katalogdienst.

Der Befehl „infacmd Idm CreateService“ verwendet die folgende Syntax:

```
CreateService
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
```

```

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ModelRepositoryService|-mrs> model_repository_service_name

<-MRSUserName|-mrsun> model_repository_service_user_name

<-MRSPassword|-mrspd> model_repository_service_user_password

[<-MRSSecurityDomain|-mrssdn> model_repository_service_user_security_domain]

[<-HttpPort|-p> port_name]

[<-HttpsPort|-sp> https_port_name]

[<-EnableTls|-tls> enable_tls true|false]

[<-KeystoreFile|-kf> keystore_file_location]

[<-KeystorePassword|-kp> keystore_password]

[<-SSLProtocol|-sslp> ssl_protocol]

<-InfaClusterServiceName|-icsn> infa_cluster_service_name

[<-isEmailEnabled|-iee> is_email_enabled true:false (default false)]

[<-OtherOptions|-oo> other options (specified in format:
[OptionGroupName.OptionName=OptionValue]. Multiple options can be separated by space.
OptionValue should be specified within double quotes if it contains a space.)]

[<-BackupNodes|-bn> node_name1,node_name2,...]

[<-isNotifyChangeEmailEnabled|-cne> is_notify_change_email_enabled true:false (default
false)]

<-EnableDataAssetAnalytics|-ed> Enable Data Asset Analytics(true, false). If you enable
this option, make sure that you configure the following parameters:
DataAssetAnalyticsDBSelect, DataAssetAnalyticsDBUsername, DataAssetAnalyticsDBPassword,
DataAssetAnalyticsDBURL

[<-DataAssetAnalyticsDBSelect|-ddt> Select the database for Data Asset Analytics
(ORACLE, SQLSERVER or POSTGRESQL)]

[<-DataAssetAnalyticsDBUsername|-ddu> Username to access the database]

[<-DataAssetAnalyticsDBPassword|-ddp> Password configured for the username]

[<-DataAssetAnalyticsDBURL|-ddl> Database connection string. Make sure that the
connection string starts with 'jdbc:informatica:']

[<-DataAssetAnalyticsDBSchema|-dds> Database schema name (applicable if you had selected
SQL Server or PostgreSQL as the database type.)]

[<-DataAssetAnalyticsSecureJDBCParameters|-dsjdbcp> Secure JDBC connection parameters]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd Idm CreateService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-NodeName -nn	node_name	Erforderlich. Knoten, auf dem der Katalogdienst ausgeführt werden soll.
-SecurityDomain  -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-ServiceName -sn	service_name	Erforderlich. Name des Katalogdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-ModelRepositoryService -mrs	model_repository_service_name	Erforderlich. Name des Modellrepository-Diensts, der dem Katalogdienst zugeordnet wird.

Option	Argument	Beschreibung
-MRSUserName -mrsun	model_repository_service_user_name	Erforderlich, wenn Sie einen Modellrepository-Dienst angeben. Benutzername für die Verbindung zum Modellrepository. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-MRSPassword -mrspd	model_repository_service_user_password	Erforderlich, wenn Sie einen Modellrepository-Dienst angeben. Benutzerpasswort für den Modellrepository-Dienst.
-MRSSecurityDomain -mrssdn	model_repository_service_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Administrator-Benutzer gehört.
-HttpPort -p	port_name	Erforderlich. Eine für einen Katalogdienstprozess verwendete eindeutige HTTP-Portnummer. Die Standardportnummer lautet 9085.
-HttpsPort -sp	https_port_name	Erforderlich, wenn Sie „Transport Layer Security aktivieren“ aktivieren. Die Portnummer für die HTTPS-Verbindung.
-EnableTls -tls	enable_tls	Wählen Sie diese Option zum Aktivieren von Transport Layer Security aus.
-KeystoreFile -kf	keystore_file_location	Erforderlich, wenn Sie „Transport Layer Security aktivieren“ auswählen. Pfad und Dateiname der Schlüsselspeicherdatei. Die Schlüsselspeicherdatei enthält die Schlüssel und Zertifikate, die bei Verwendung des SSL-Sicherheitsprotokolls mit Catalog Administrator erforderlich sind.
-KeystorePassword -kp	keystore_password	Erforderlich, wenn Sie „Transport Layer Security aktivieren“ auswählen. Das Passwort für die Schlüsselspeicherdatei.
-SSLProtocol -sslp	ssl_protocol	Optional. Zu verwendendes Secure Sockets Layer-Protokoll.
-InfaClusterServiceName -icsn	infa_cluster_service_name	Erforderlich. Name des Informatica-Cluster-Diensts.



Option	Argument	Beschreibung
-isEmailEnabled -iee	is_email_enabled	Optional. Geben Sie „True“ an, wenn Sie die E-Mail-Benachrichtigung aktivieren möchten. Standardwert ist „False“.
-OtherOptions -oo	other options	Optional. Geben Sie Name-Wert-Paare durch Leerzeichen getrennt ein. Zur Eingabe eines Optionswerts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Backup-Knoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.
-isNotifyChangeEmailEnabled -cne	is_notify_change_email_enabled	Optional. Legen Sie „True“ fest, wenn Sie Benachrichtigungen zu Objektänderungen aktivieren möchten. Standardwert ist „False“.
-EnableDataAssetAnalytics -ed	Data Asset Analytics aktivieren („true“, „false“)	Erforderlich. Geben Sie „true“ an, wenn Sie Data Asset Analytics mit Enterprise Data Catalog aktivieren möchten. Wenn Sie diese Option aktivieren, müssen Sie die folgenden Parameter konfigurieren: <ul style="list-style-type: none"> <li>- DataAssetAnalyticsDBSelect</li> <li>- DataAssetAnalyticsDBUsername</li> <li>- DataAssetAnalyticsDBPassword</li> <li>- DataAssetAnalyticsDBURL</li> </ul>
-DataAssetAnalyticsDBSelect -ddt	Datenbank für Data Asset Analytics auswählen (ORACLE, SQLSERVER oder POSTGRESQL)	Erforderlich, wenn der Wert der Option <code>EnableDataAssetAnalytics</code> auf „true“ festgelegt wird. Gilt für die folgenden Datenbanken: <ul style="list-style-type: none"> <li>- Oracle</li> <li>- SQL Server</li> <li>- PostgreSQL</li> </ul>
-DataAssetAnalyticsDBUsername -ddu	Benutzername für den Zugriff auf die Datenbank.	Erforderlich, wenn der Wert der Option <code>EnableDataAssetAnalytics</code> auf „true“ festgelegt wird. Geben Sie den Benutzernamen für den Zugriff auf die Datenbank für Data Asset Analytics an.

Option	Argument	Beschreibung
DataAssetAnalyticsDBPassword -ddp	Für den Benutzernamen konfiguriertes Passwort.	Erforderlich, wenn der Wert der Option <code>EnableDataAssetAnalytics</code> auf „true“ festgelegt wird. Geben Sie das Passwort für den Zugriff auf die Datenbank für Data Asset Analytics an.
DataAssetAnalyticsDBURL -ddl	Verbindungszeichenfolge der Datenbank	Erforderlich, wenn der Wert der Option <code>EnableDataAssetAnalytics</code> auf „true“ festgelegt wird. Geben Sie die Verbindungszeichenfolge der Datenbank an. Stellen Sie sicher, dass die Verbindungszeichenfolge mit 'jdbc:informatica:' beginnt.
DataAssetAnalyticsDBSchema -dds	Datenbank-Schemaname	Optional. Geben Sie den Schemanamen der Datenbank an. Anwendbar, wenn Sie als Datenbanktyp „SQL Server“ oder „PostgreSQL“ ausgewählt haben.
DataAssetAnalyticsSecureJDBCParameters -dsjdbcp	Sichere JDBC-Verbindungsparameter	Optional. Wenn die Datenbank für Data Asset Analytics mittels SSL-Protokoll gesichert wird, müssen Sie die sicheren Datenbankparameter eingeben. Geben Sie die Parameter in Form von Schlüssel-Wert-Paaren ein, die durch ein Semikolon getrennt sind. Beispiel: <code>param1=value1;param2=value2</code>

## ListServiceOptions

Listet Dienstoptionen für den Katalogdienst auf.

Der Befehl „`infacmd Idm ListServiceOptions`“ verwendet die folgende Syntax:

```
ListServiceOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd Idm ListServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Katalogdiensts.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

# ListServiceProcessOptions

Listet Dienstprozessoptionen für den Catalog Administrator-Prozess auf.

Der Befehl „infacmd Idm ListServiceProcessOptions“ verwendet die folgende Syntax:

```
ListServiceProcessOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für infacmd Idm ListServiceProcessOptions beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Katalogdiensts.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-NodeName -nn	node_name	<p>Erforderlich. Erforderlich. Name des Knotens, auf dem der Dienstprozess ausgeführt wird.</p>

## migrateContents

Migriert Inhalte. Geben Sie das Eingabeverzeichnis an, aus dem Sie den Inhalt migrieren oder überprüfen möchten. Führen Sie den Befehl migrateContents aus, wenn der Katalogdienst, der Informatica-Cluster-Dienst und die erforderlichen Speicher aktiviert sind. Vor dem Migrieren der Katalogdaten müssen Sie die folgenden Umgebungsvariablen festlegen

- **INFA\_TRUSTSTORE.** Mithilfe des folgenden Beispielbefehls können Sie die Variable festlegen: `export INFA_TRUSTSTORE= <Speicherort der Informatica-Truststore-Datei>.` Standardspeicherort ist `$INFA_HOME/services/shared/security.`
- **INFA\_KEYSTORE.** Mithilfe des folgenden Beispielbefehls können Sie die Variable festlegen: `export INFA_KEYSTORE=<Speicherort der Schlüsselspeicherdatei>.` Standardspeicherort ist `$INFA_HOME/services/shared/security.` Diese Variable ist nur erforderlich, wenn Sie eine Konfiguration mit benutzerdefinierter SSL für die Informatica-Domäne verwendet haben. Für Konfigurationen mit Standard-SSL und ohne SSL müssen Sie die Variable aufheben.
- **Verschlüsseltes INFA\_TRUSTSTORE\_PASSWORD.** Verschlüsseln Sie das von Ihnen festgelegte Passwort. Mithilfe des folgenden Beispielbefehls können Sie das verschlüsselte Passwort festlegen: `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA==".`

- Verschlüsseltes INFA\_KEYSTORE\_PASSWORD. Verschlüsseln Sie das von Ihnen festgelegte Passwort. Mithilfe des folgenden Beispielbefehls können Sie das verschlüsselte Passwort festlegen: `export INFA_KEYSTORE_PASSWORD="6cDE/ItyUL/Rtui9nhVRI=="`. Diese Variable ist nur erforderlich, wenn Sie eine Konfiguration mit benutzerdefinierter SSL für die Informatica-Domäne verwendet haben. Für Konfigurationen mit Standard-SSL und ohne SSL müssen Sie die Variable aufheben.

**Hinweis:** Siehe Beispielbefehl zum Verschlüsseln des Passworts: `$INFA_HOME/server/bin/pmpasswd <Passwort>`

Beispiel:

- `export INFA_KEYSTORE_PASSWORD=hQDP8O8tfwxRSwbeANEptl4AIQqJcSj9ZMDkVK+9S+Y=`
- `export INFA_TRUSTSTORE_PASSWORD=hx/nRWisSjnQ0zEGV3N7j1FCGF0m5RfisQxKTdf5f8Y=`
- `export INFA_TRUSTSTORE=/data/Informatica/LDM1051/services/shared/security/`
- `export INFA_KEYSTORE=/data/Informatica/LDM1051/services/shared/security`

Beachten Sie vor der Ausführung dieses Befehls die folgenden Punkte:

- Für den Befehl `migrateContents` sind die Umgebungsvariablen `INFA_KEYSTORE` und `INFA_KEYSTORE_PASSWORD` erforderlich, um eine Verbindung zu den Solr- und MongoDB-Diensten des Informatica-Cluster-Diensts herzustellen.
- Die Administratorbenutzer oder Benutzer, die Teil der Administratorgruppe sind, können den Befehl `migrateContents` ausführen.
- Um den Befehl „`migrateContents`“ vom Sicherungsknoten für den Katalogdienst auszuführen, müssen Sie passwortloses SSH zwischen dem Sicherungsknoten und allen Knoten im Cluster aktivieren.
- Legen Sie die Umgebungsvariablen `INFA_TRUSTSTORE` und `INFA_TRUSTSTORE_PASSWORD` für die Informatica-Domäne sowohl mit als auch ohne SSL fest.

Der Befehl „`infacmd ldm migrateContents`“ verwendet die folgende Syntax:

```
LDM migrateContents

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-InputDirectory|-id> full path to backup directory. For eg. - /backup/export

[<-Resume> This is to resume migrating contents from the last checkpoint available. If
set to false, migration will start from scratch.]

[<-Force> This is to forcefully launch another migration process ignoring the lock held
by previous process.]

[<-Verify> This is to verify restored data after migration is complete.]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd Idm migrateContents“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Katalogdiensts.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-InputDirectory -id	Eingabeverzeichnis	<p>Vollständiger Pfad zum Sicherungsverzeichnis. Beispiel: - /backup/export</p>
-Resume	resume	<p>Verwenden Sie diese Option, um die Migration von Inhalten ab dem letzten verfügbaren Prüfpunkt fortzusetzen. Wenn als Wert „False“ festgelegt wird, beginnt die Migration von vorne.</p>
-Force	force	<p>Verwenden Sie diese Option, um das Starten eines weiteren Migrationsprozesses zu erzwingen, indem die vom vorherigen Prozess gesetzte Sperre ignoriert wird.</p>
-Verify	verify	<p>Verwenden Sie diese Option, um wiederhergestellte Daten nach Abschluss der Migration zu überprüfen.</p>



# publishArchive

Erstellt eine Ressource im Offline-Modus und führt den Scan aus.

Der Befehl „infacmd Idm publishArchive“ verwendet folgende Syntax:

```
publishArchive
<-DomainName|-dn> Fully qualified domain name
<-UserName|-un> user_name
<-Password|-pd> The Encrypted user password to access the ISP
<-ServiceName|-sn> Name of the Catalog Service
<-ResourceName|-rn> Name of the resource
[<-SecurityDomain|-sd> Name of the security domain]
<-DomainHost|-dh> Name of the host machine where the domain runs
<-DomainPort|-dp> Port number of the domain
[<-DomainSslEnabled|-dse> is domain SSL enabled]
[<-SslLocation|-ts> Path to the truststore]
[<-SslPassword|-tsp> Password to access the truststore]
<-ArchiveFilePath|-arf> Path to the metadata archive file
[<-Verbose|-v> Verbose]
[<-WaitToCatalog|-w> Wait for the metadata ingestion to catalog to complete]
[<-Force|-f> Force resource creation or update]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd Idm CreateService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/ Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Katalogdiensts.
-ResourceName -rn	Name der Ressource.	Erforderlich. Name der Ressource. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, manuelle Zeilenumbrüche bzw. Absatzmarken oder Tabstoppzeichen noch die folgenden Zeichen enthalten: \ / * ? < > "   \$
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-DomainHost -dh	Name des Domänenhosts	Erforderlich. Name des Hostcomputers, auf dem die Domäne ausgeführt wird.
-DomainPort -dp	Portnummer für die Domäne	Erforderlich. Die Portnummer der Domäne.
-DomainSslEnabled -dse	is_Domain_SSL_Enabled	Optional. Geben Sie „True“ an, um die SSL-Domäne zu aktivieren. Standardwert ist „False“.
-SslLocation -ts	-	Optional. Pfad zum Truststore.
-SslPassword -tsp	-	Optional. Passwort für den Zugriff auf den Truststore.
-ArchiveFilePath -arf	-	Erforderlich. Pfad zur Metadatenarchivdatei.

Option	Argument	Beschreibung
-Verbose -v	Verbose	Optional. Zeigt oder speichert Bereinigungsinformationen im Verbose-Modus. Verbose-Modus bietet ausführliche Informationen zu Objektversionen, einschließlich Repository-Name, Ordner-Name, Versionsnummer und Status. Sie können die Option -b mit -o und -p verwenden.
-WaitToCatalog -w	-	Optional. Wartet auf den Abschluss der Metadatenerfassung im Katalog.
-Force -f	-	Optional. Erstellt oder aktualisiert die Ressource.

## restoreContents

Stellt die Katalogdaten wieder her.

Vor dem Wiederherstellen der Katalogdaten müssen Sie die folgenden Umgebungsvariablen festlegen:

- **INFA\_TRUSTSTORE.** Mithilfe des folgenden Beispielbefehls können Sie die Variable festlegen: `export INFA_TRUSTSTORE= <Speicherort der Informatica-Truststore-Datei>.` Standardspeicherort ist `$INFA_HOME/services/shared/security`.
- **INFA\_KEYSTORE.** Mithilfe des folgenden Beispielbefehls können Sie die Variable festlegen: `export INFA_KEYSTORE=<Speicherort der Schlüsselspeicherdatei>.` Standardspeicherort ist `$INFA_HOME/services/shared/security`. Diese Variable ist nur erforderlich, wenn Sie eine Konfiguration mit benutzerdefinierter SSL für die Informatica-Domäne verwendet haben. Für Konfigurationen mit Standard-SSL und ohne SSL müssen Sie die Variable aufheben.
- **Verschlüsseltes INFA\_TRUSTSTORE\_PASSWORD.** Verschlüsseln Sie das von Ihnen festgelegte Passwort. Mithilfe des folgenden Beispielbefehls können Sie das verschlüsselte Passwort festlegen: `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA==".`
- **Verschlüsseltes INFA\_KEYSTORE\_PASSWORD.** Verschlüsseln Sie das von Ihnen festgelegte Passwort. Mithilfe des folgenden Beispielbefehls können Sie das verschlüsselte Passwort festlegen: `export INFA_KEYSTORE_PASSWORD="6cDE/ItyUL/Rtui9nhVRI==".` Diese Variable ist nur erforderlich, wenn Sie eine Konfiguration mit benutzerdefinierter SSL für die Informatica-Domäne verwendet haben. Für Konfigurationen mit Standard-SSL und ohne SSL müssen Sie die Variable aufheben.

**Hinweis:** Siehe Beispielbefehl zum Verschlüsseln des Passworts: `$INFA_HOME/server/bin/pmpasswd <Passwort>`

Beispiel:

- `export INFA_KEYSTORE_PASSWORD=hQDP808tfwxRSwbeANEptl4AIQqJcSj9ZMDkVK+9S+Y=`
- `export INFA_TRUSTSTORE_PASSWORD=hx/nRWisSjnQ0zEGV3N7j1FCGF0m5RfisQxKTdf5f8Y=`
- `export INFA_TRUSTSTORE=/data/Informatica/LDM1051/services/shared/security/`
- `export INFA_KEYSTORE=/data/Informatica/LDM1051/services/shared/security`

Beachten Sie vor der Ausführung dieses Befehls die folgenden Punkte:

- Für den Befehl `restoreContents` sind die Umgebungsvariablen `INFA_KEYSTORE` und `INFA_KEYSTORE_PASSWORD` erforderlich, um eine Verbindung zu den Solr- und MongoDB-Diensten des Informatica-Cluster-Diensts herzustellen.
- Sie sollten den Befehl `restoreContents` nicht verwenden, um eine Knotensicherung im Setup mit mehreren Knoten wiederherzustellen. Die Einschränkung gilt für die Wiederherstellungsoption „SEARCH store“.
- Legen Sie die Umgebungsvariablen `INFA_TRUSTSTORE` und `INFA_TRUSTSTORE_PASSWORD` für die Informatica-Domäne sowohl mit als auch ohne SSL fest.
- Wenn Solr in einer Konfiguration mit mehreren Knoten installiert ist, müssen Sie die Option `ClusterSharedFilesystemPath` im Informatica-Cluster-Dienst zum Wiederherstellen von Solr verwenden.

Sie können Katalogdaten aus der aktuellen Version nicht verwenden, um Daten für eine frühere Version wiederherzustellen. Wenn Sie jedoch eine kumulative Patch-Version oder ein Service Pack angewendet haben, können Sie die vorhandenen Katalogdaten zum Wiederherstellen der Daten für eine frühere Version verwenden.

Sie müssen sicherstellen, dass die Basisversionen für die vorhandene und die vorherige Version identisch sind.

Der Befehl `infacmd Idm restoreContents` verwendet die folgende Syntax:

```
restoreContents

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-InputFileName|-if> input_file_name (Complete path of backup ZIP file on local machine.
The content of ZIP file will be copied to cluster.)

[<-Force|-fr> force(This is to forcefully clean the existing contents of cluster where
data is to be restored and restore the backup data from scratch)]
```

In der folgenden Tabelle werden die Optionen und Argumente für `infacmd Idm restoreContents` beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Katalogdiensts.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Beim Namen der Sicherheitsdomäne wird zwischen Groß- und Kleinschreibung unterschieden. Wenn für die Domäne die native oder LDAP-Authentifizierung verwendet wird, ist „Nativ“ der Standardwert. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der <code>infacmd</code> versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-InputFileName -if	input_file_name	Erforderlich. Vollständiger Pfad der ZIP-Backup-Datei auf dem Host des Katalogdiensts.
-Force -fr	force	Optional. Verwenden Sie diese Option, um die Bereinigung des vorhandenen Inhalts des Informatica-Clusters, in dem Daten wiederhergestellt werden sollen, zu erzwingen und die Sicherungsdaten von Grund auf neu zu erstellen.  Wenn der SEARCH-Speicher nicht in der Sicherung enthalten ist, müssen Sie den Informatica-Cluster-Dienst recyceln und anschließend den Katalogdienst neu indizieren, um die Daten für Apache Solr aufzufüllen.

Ab Enterprise Data Catalog 10.5.1.1 können Sie den Status des Wiederherstellungsvorgangs in der folgenden Protokolldatei auf dem Knoten anzeigen, auf dem Sie den Befehl ausführen: `<Informatica installation directory>/logs/<Node name>/services/CatalogService/<Catalog Service name>/LDMRestore.log`. Die maximale Dateigröße für jede Protokolldatei beträgt 100 MB. Nach Erreichen der maximalen Dateigröße wird eine neue Datei erstellt. Maximal 20 Protokolldateien können gespeichert werden. Nach Erreichen dieses Grenzwerts wird die älteste Protokolldatei durch die neueste Protokolldatei ersetzt.

## UpdateServiceOptions

Aktualisiert Optionen für den Katalogdienst. Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Der Befehl „`infacmd Idm UpdateServiceOptions`“ verwendet die folgende Syntax:

```
UpdateServiceOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-Options|-o> options]
[<-PrimaryNode|-nn> node_name]
[<-BackupNodes|-bn> node_name1,node_name2,...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd Idm UpdateServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Katalogdiensts.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-Options -o	options	<p>Optional. Geben Sie Name-Wert-Paare durch Leerzeichen getrennt ein.</p> <p>Wenn Sie Service Pack 10.5.1.1 oder eine spätere Version angewendet haben, können Sie das SSL-Protokoll für den Katalogdienst mithilfe der Option <code>GeneralOptions.SSLProtocol</code> auf TLS 1.1 oder TLS 1.2 konfigurieren. Geben Sie einen der folgenden Werte an:</p> <ul style="list-style-type: none"> <li>- TLSv1.1</li> <li>- TLSv1.2</li> </ul> <p>Sie können die folgenden, auf Data Asset Analytics bezogenen Optionen aktualisieren:</p> <ul style="list-style-type: none"> <li>- <code>DAARepository.EnableDataAssetAnalytics</code>: Geben Sie <code>True</code> an, um Data Asset Analytics zu aktivieren.</li> <li>- <code>DAARepository.DataAssetAnalyticsDBSelect</code>: Geben Sie eine der folgenden Datenbanken an: <ul style="list-style-type: none"> <li>- Oracle</li> <li>- SQL Server</li> <li>- PostgreSQL</li> </ul> </li> <li>- <code>DAARepository.DataAssetAnalyticsDBUsername</code>: Geben Sie den Benutzernamen für den Zugriff auf die Data Asset Analytics-Datenbank an.</li> <li>- <code>DAARepository.DataAssetAnalyticsDBPassword</code>: Geben Sie das Passwort für den Zugriff auf die Data Asset Analytics-Datenbank an.</li> <li>- <code>DAARepository.DataAssetAnalyticsDBURL</code>: Geben Sie die Verbindungszeichenfolge der Datenbank an.</li> <li>- <code>DAARepository.DataAssetAnalyticsDBSchema</code>: Geben Sie den Schemanamen der Datenbank an.</li> <li>- <code>DAARepository.DataAssetAnalyticsSecureJDBCParameters</code>: Geben Sie die JDBC-Parameter an. Beispiel: <code>param1=value1;param2=value2</code></li> </ul>
-PrimaryNode -nn	node_name	Optional. Wenn Sie hohe Verfügbarkeit für Enterprise Data Catalog konfigurieren möchten, geben Sie den Namen des Primärknotens an.
-BackupNodes -bn	node_names	Wenn Sie optional hohe Verfügbarkeit für Enterprise Data Catalog konfigurieren möchten, geben Sie eine Liste mit kommagetrennten Sicherungsknotennamen an.

## UpdateServiceProcessOptions

Aktualisiert die Prozessoptionen für den Katalogdienst. Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Der Befehl „`infacmd Idm UpdateServiceProcessOptions`“ verwendet die folgende Syntax:

```
UpdateServiceProcessOptions
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
<-UserName|-un> user_name
```



```

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Options|-o> options

```

In der folgenden Tabelle werden die Optionen und Argumente für infacmd Idm UpdateServiceProcessOptions beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienstprozess ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Katalogdiensts.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-Options -o	options	<p>Erforderlich. Geben Sie Name-Wert-Paare durch Leerzeichen getrennt ein.</p>

## upgrade

Aktualisiert den Katalogdienst. Wenn SSL für den Katalogdienst aktiviert ist, müssen Sie die folgenden Umgebungsvariablen festlegen, bevor Sie den Inhalt wiederherstellen:

- **INFA\_TRUSTSTORE.** Mithilfe des folgenden Beispielbefehls können Sie die Variable festlegen: `export INFA_TRUSTSTORE= <Speicherort der Informatica-Truststore-Datei>`. Standardspeicherort ist `$INFA_HOME/services/shared/security`.
- **INFA\_KEYSTORE.** Mithilfe des folgenden Beispielbefehls können Sie die Variable festlegen: `export INFA_KEYSTORE=<Speicherort der Schlüsselspeicherdatei>`. Standardspeicherort ist `$INFA_HOME/services/shared/security`. Diese Variable ist nur erforderlich, wenn Sie eine Konfiguration mit benutzerdefinierter SSL für die Informatica-Domäne verwendet haben. Für Konfigurationen mit Standard-SSL und ohne SSL müssen Sie die Variable aufheben.
- **Verschlüsseltes INFA\_TRUSTSTORE\_PASSWORD.** Verschlüsseln Sie das von Ihnen festgelegte Passwort. Mithilfe des folgenden Beispielbefehls können Sie das verschlüsselte Passwort festlegen: `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA=="`.
- **Verschlüsseltes INFA\_KEYSTORE\_PASSWORD.** Verschlüsseln Sie das von Ihnen festgelegte Passwort. Mithilfe des folgenden Beispielbefehls können Sie das verschlüsselte Passwort festlegen: `export INFA_KEYSTORE_PASSWORD="6cDE/ItyUL/Rtui9nhVRI=="`. Diese Variable ist nur erforderlich, wenn Sie eine Konfiguration mit benutzerdefinierter SSL für die Informatica-Domäne verwendet haben. Für Konfigurationen mit Standard-SSL und ohne SSL müssen Sie die Variable aufheben.

**Hinweis:** Mithilfe des folgenden Beispielbefehls können Sie das verschlüsselte Passwort festlegen: \$INFA\_HOME/server/bin/prmpasswd <password>

Beispiel:

- export INFA\_KEYSTORE\_PASSWORD=hQDP8O8tfwxRSwbeANEptl4AIQqJcSj9ZMDkVK+9S+Y=
- export INFA\_TRUSTSTORE\_PASSWORD=hx/nRWisSjnQ0zEGV3N7j1FCGF0m5RfisQxKTdf5f8Y=
- export INFA\_TRUSTSTORE=/data/Informatica/LDM1051/services/shared/security/
- export INFA\_KEYSTORE=/data/Informatica/LDM1051/services/shared/security

**Hinweis:** Legen Sie die Umgebungsvariablen INFA\_TRUSTSTORE und INFA\_TRUSTSTORE\_PASSWORD für die Informatica-Domäne sowohl mit als auch ohne SSL fest.

Der Befehl „infacmd ldm upgrade“ verwendet die folgende Syntax:

```
upgrade
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ldm upgrade“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Katalogdiensts.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## KAPITEL 23

# infacmd mas-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [CreateService, 849](#)
- [ListServiceOptions, 853](#)
- [ListServiceProcessOptions, 855](#)
- [UpdateServiceOptions, 857](#)
- [UpdateServiceProcessOptions, 860](#)

## CreateService

Erstellt einen Metadaten-Zugriffsdienst. Der Metadaten-Zugriffsdienst ist ein Anwendungsdienst, mit dem das Developer Tool auf Hadoop-Verbindungsinformationen zugreifen kann, um Metadaten zu importieren und in der Vorschau anzuzeigen.

Der Befehl „infacmd mas CreateService“ verwendet die folgende Syntax:

```
CreateService

<-DomainName|-dn> DomainName

<-NodeName|-nn> NodeName

<-UserName|-un> Username

<-Password|-pd> Password

<-ServiceName|-sn> ServiceName

<-HTTPProtocolType|-hp> HTTPProtocolType

[<-HTTPPort|-pt> HTTPPort]

[<-HTTPSPort|-spt> HTTPSPort]

[<-HadoopServicePrincipalName|-hpn> HadoopServicePrincipalName]

[<-HadoopKeyTab|-hkt> HadoopKeyTab]

[<-ServiceDescription|-sd> ServiceDescription]

[<-ResilienceTimeout|-re> ResilienceTimeout]

[<-FolderPath|-fp> FolderPath]

[<-BackupNodes|-bn> BackupNodes]
```

```
[<-KeyStoreFile|-kf> KeyStoreFile]
[<-KeystorePassword|-kp> KeystorePassword]
[<-TruststoreFile|-tf> TruststoreFile]
[<-TruststorePassword|-tp> TruststorePassword]
[<-SecurityDomain|-sdn> SecurityDomain]
[<-SSLProtocol|-sp> SSLProtocol]
[<-loggedInUserAsImpersonationUser|-uiu> UseLoggedInUserAsImpersonationUser]
[<-enableOSProfile|-osp> EnableOSProfile]
```

In der folgenden Tabelle werden die Optionen und Argumente für `infacmd mas CreateService` beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-NodeName -nn	node_name	Knoten, auf dem der Metadaten-Zugriffsdienst ausgeführt wird. Sie können den Datenintegrationsdienst nur auf einem Knoten ausführen.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Metadaten-Zugriffsdiensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositories kompatibel sein. Der Name darf maximal 230 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten:  / * ? < > "

Option	Argument	Beschreibung
-HTTPProtocolType -hp	http_protocol_type	<p>Sicherheitsprotokoll, das der Metadaten-Zugriffsdienst verwendet. Geben Sie einen der folgenden Werte ein:</p> <ul style="list-style-type: none"> <li>- HTTP. In Anfragen an den Dienst muss eine HTTP-URL verwendet werden..</li> <li>- HTTPS. In Anfragen an den Dienst muss eine HTTPS-URL verwendet werden.</li> </ul> <p>Wenn Sie den HTTP-Protokolltyp auf HTTPS setzen, aktivieren Sie auch Transport Layer Security (TLS) für den Dienst.</p> <p>Standardwert ist HTTP.</p>
-HTTPPort -pt	http_port	<p>Erforderlich, wenn Sie keinen HTTPS-Port angeben. Eindeutige HTTP-Portnummer, die für die einzelnen Prozesse des Metadaten-Zugriffsdiensts verwendet wird. Nachdem Sie den Dienst erstellt haben, können Sie für jeden Prozess des Metadaten-Zugriffsdiensts eine eigene Portnummer definieren.</p> <p>Standardwert ist 7080. Der Metadaten-Zugriffsdienst verwendet aufeinanderfolgende Portnummern, um mehrere Hadoop-Distributionen zu verbinden.</p>
-HTTPSPort -SPT	https_port	<p>Erforderlich, wenn Sie keinen HTTP-Port angeben. Eindeutige HTTPS-Portnummer, die für die einzelnen Prozesse des Metadaten-Zugriffsdiensts verwendet wird. Nachdem Sie den Dienst erstellt haben, können Sie für jeden Prozess des Metadaten-Zugriffsdiensts eine eigene Portnummer definieren.</p> <p>Der Metadaten-Zugriffsdienst verwendet aufeinanderfolgende Portnummern, um mehrere Hadoop-Distributionen zu verbinden.</p>
- HadoopServicePrincipalName -hpn	hadoop_spn	<p>Dienstprinzipalname (SPN) des Metadaten-Zugriffsdiensts zum Herstellen einer Verbindung mit einem Hadoop-Cluster, der Kerberos-Authentifizierung verwendet.</p> <p>Nicht anwendbar für die MapR-Distribution.</p>
-HadoopKeyTab -hkt	keytab_file_path	<p>Der Dateipfad der Keytab-Datei von Kerberos auf dem Computer, auf dem der Metadaten-Zugriffsdienst ausgeführt wird.</p> <p>Nicht anwendbar für die MapR-Distribution.</p>
-ServiceDescription -sd	service_description	Optional. Dienstbeschreibung.
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

Option	Argument	Beschreibung
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domännennamen) des Ordners, in dem der Metadaten-Zugriffsdienst erstellt werden soll. Folgendes Format ist erforderlich: /parent_folder/child_folder Standardwert ist „/“ (die Domäne).
-BackupNodes -bn	node_name1,node_name 2,...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Backup-Knoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.
-KeystoreFile -kf	keystore_file_location	Pfad und Dateiname der Schlüsselspeicherdatei, die die Schlüssel und Zertifikate enthält, die zur Verwendung des HTTPS-Protokolls für den Metadaten-Zugriffsdienst erforderlich sind. Sie können eine Schlüsselspeicherdatei mit einem Keytool erstellen. Bei Keytool handelt es sich um ein Dienstprogramm, das private oder öffentliche Schlüsselpaare und zugeordnete Zertifikate in einer Schlüsselspeicherdatei erzeugt und speichert. Sie können das selbstsignierte Zertifikat nutzen oder ein Zertifikat verwenden, das von einer Zertifizierungsstelle signiert wurde.
-KeystorePassword -kp	keystore_password	Passwort für die Schlüsselspeicherdatei.
-TruststoreFile -tf	trust_store_file	Erforderlich, wenn bei der Domäne SSL aktiviert ist. Domänenspeicherort der Truststore-Datei im Cluster.
-TruststorePassword -tp	trust_store_password	Erforderlich, wenn bei der Domäne SSL aktiviert ist. Passwort der Truststore-Domäne.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomännennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-SSLProtocol -sp	ssl_protocol	Optional. Zu verwendendes Secure Sockets Layer-Protokoll.



Option	Argument	Beschreibung
-HadoopImpersonationUser -hu	hadoop_impersonation_user	Optional. Geben Sie einen Benutzernamen ein, dessen Identität vom Metadaten-Zugriffsdienst übernommen werden soll, wenn eine Verbindung mit einer Hadoop-Umgebung hergestellt wird.
-loggedInUserAsImpersonationUser -uiu	use_logged_in_user_as_proxy	Erforderlich, wenn der Hadoop-Cluster die Kerberos-Authentifizierung verwendet. Hadoop-Identitätswechselbenutzer. Der Benutzername, dessen Identität vom Metadaten-Zugriffsdienst übernommen wird, um Metadaten zur Entwurfszeit aus der Hadoop-Umgebung zu importieren.
-enableOSProfile -osp	enable_OS_profile	Gibt an, dass der Metadaten-Zugriffsdienst Betriebssystemprofile für die Vorschau der Metadaten verwenden kann. Standardwert ist „False“.

## ListServiceOptions

Listet die Eigenschaften für einen Metadaten-Zugriffsdienst auf.

Der Befehl „infacmd mas ListServiceOptions“ verwendet die folgende Syntax:

```
ListServiceOptions
<-DomainName|-dn> DomainName
<-UserName|-un> Username
<-Password|-pd> Password
<-ServiceName|-sn> ServiceName
[<-SecurityDomain|-sdn> SecurityDomain]
[<-ResilienceTimeout|-re> ResilienceTimeout]
```

In der folgenden Tabelle werden die Optionen und Argumente für `infacmd mas ListServiceOptions` beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Metadaten-Zugriffsdiensts.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## ListServiceProcessOptions

Listet die Eigenschaften eines Metadaten-Zugriffsdienst-Prozesses auf.

Der Befehl „infacmd mas ListServiceProcessOptions“ verwendet die folgende Syntax:

```
ListServiceProcessOptions
<-DomainName|-dn> DomainName
<-NodeName|-nn> NodeName
<-UserName|-un> Username
<-Password|-pd> Password
<-ServiceName|-sn> ServiceName
[<-SecurityDomain|-sdn> SecurityDomain]
[<-ResilienceTimeout|-re> ResilienceTimeout]
```

In der folgenden Tabelle werden die Optionen und Argumente für `infacmd mas ListServiceProcessOptions` beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienstprozess ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Metadaten-Zugriffsdiensts.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## UpdateServiceOptions

Aktualisiert die Eigenschaften des Metadaten-Zugriffsdiensts. Führen Sie zum Anzeigen der aktuellen Eigenschaften den Befehl „infacmd mas ListServiceOptions“ aus.

Sie können die Eigenschaften ändern, während der Dienst ausgeführt wird, aber Sie müssen den Dienst neu starten, damit die geänderten Eigenschaften wirksam werden.

Der Befehl „infacmd mas UpdateServiceOptions“ verwendet die folgende Syntax:

```
UpdateServiceOptions
<-DomainName|-dn> DomainName
<-UserName|-un> Username
<-Password|-pd> Password
<-ServiceName|-sn> ServiceName
[<-SecurityDomain|-sdn> SecurityDomain]
[<-ResilienceTimeout|-re> ResilienceTimeout]
[<-Options|-o> options]
<-PrimaryNode|-nn> PrimaryNodeName
```

```
[<-BackupNodes|-bn> node_name1,node_name2,...]
```

```
[<-SearchIndexRoot|-si> SearchIndexRoot]
```

In der folgenden Tabelle werden die Optionen und Argumente für `infacmd mas UpdateServiceOptions` beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Metadaten-Zugriffsdiensts, dem die Anwendung bereitgestellt wird.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Options -o	options	Optional. Geben Sie jede Option durch ein Leerzeichen getrennt ein. Führen Sie zum Anzeigen der Optionen den Befehl „infacmd mas ListServiceOptions“ aus.
-PrimaryNode -nn	node_name	Geben Sie den Knoten ein, auf dem der Metadaten-Zugriffsdienst ausgeführt wird. Der Metadaten-Zugriffsdienst kann nur auf einem Knoten ausgeführt werden.
-BackupNodes -bn	node_name1,node_name2,.. ..	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Backup-Knoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.
-SearchIndexRoot -si	search_index_root	Optional. Ändert das Verzeichnis für den Suchindex. Geben Sie den vollständigen Pfad zum Verzeichnis ein. Standardmäßig wird das Informatica-Installationsverzeichnis verwendet.

## Metadaten-Zugriffsdienst-Optionen

Verwenden Sie die Metadaten-Zugriffsdienstoptionen mit dem Befehl „infacmd mas UpdateServiceOptions“.

Geben Sie die Optionen für den Metadaten-Zugriffsdienst im folgenden Format ein:

```
... -o option_type.option_name=value
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Optionen für den Metadaten-Zugriffsdienst beschrieben:

Option	Beschreibung
ExecutionContextOptions.HadoopDistribution	Das Hadoop-Distributionsverzeichnis auf dem Knoten des Metadaten-Zugriffsdiensts. Der Inhalt des Hadoop-Distributionsverzeichnisses des Metadaten-Zugriffsdiensts muss mit dem Inhalt des Hadoop-Distributionsverzeichnisses auf den Datenknoten identisch sein. Geben Sie <Informatica-Installationsverzeichnis>/Informatica/services/shared/hadoop/[Hadoop_distribution_name] ein.
HttpConfigurationOptions.HTTPProtocolType	Sicherheitsprotokoll, das der Metadaten-Zugriffsdienst verwendet. Geben Sie einen der folgenden Werte ein: <ul style="list-style-type: none"> <li>- HTTP. In Anfragen an den Dienst muss eine HTTP-URL verwendet werden..</li> <li>- HTTPS. In Anfragen an den Dienst muss eine HTTPS-URL verwendet werden.</li> </ul> Wenn Sie den HTTP-Protokolltyp auf HTTPS setzen, aktivieren Sie auch Transport Layer Security (TLS) für den Dienst. Standardwert ist HTTP.
MASProperties.EnableOSProfile	Flag zur Angabe, dass der Metadaten-Zugriffsdienst Betriebssystemprofile für die Metadaten-Vorschau verwenden kann. Standardwert ist „False“.
MASProperties.HadoopKeytab	Der Dateipfad der Keytab-Datei von Kerberos auf dem Computer, auf dem der Metadaten-Zugriffsdienst ausgeführt wird. Nicht anwendbar für die MapR-Distribution.
MASProperties.HadoopPrincipal	Dienstprinzipalname (SPN) des Metadaten-Zugriffsdiensts zum Herstellen einer Verbindung mit einem Hadoop-Cluster, der Kerberos-Authentifizierung verwendet. Nicht anwendbar für die MapR-Distribution.
MASProperties.LoggedInUserAsImperUser	Erforderlich, wenn der Hadoop-Cluster Kerberos-Authentifizierung verwendet.

## UpdateServiceProcessOptions

Aktualisiert die Eigenschaften eines Metadaten-Zugriffsdienst-Prozesses. Führen Sie zum Anzeigen der aktuellen Eigenschaften den Befehl „`infacmd mas ListServiceProcessOptions`“ aus.

Geben Sie die Optionen in folgendem Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Der Befehl „`infacmd mas UpdateServiceProcessOptions`“ verwendet die folgende Syntax:

```
UpdateServiceProcessOptions
<-DomainName|-dn> DomainName
<-NodeName|-nn> NodeName
```



```

<-UserName|-un> Username

<-Password|-pd> Password

<-ServiceName|-sn> ServiceName

[<-SecurityDomain|-sdn> SecurityDomain]

[<-ResilienceTimeout|-re> ResilienceTimeout]

```

In der folgenden Tabelle werden die Optionen und Argumente für infacmd mas UpdateServiceProcessOptions beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
NodeName -nn	node_name	Erforderlich. Knoten, auf dem der Metadaten-Zugriffsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Metadaten-Zugriffsdiensts.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## Optionen für Metadaten-Zugriffsdienst-Prozesse

Verwenden Sie die Optionen für Metadaten-Zugriffsdienst-Prozesse mit dem Befehl „infacmd mas UpdateServiceProcessOptions“.

Geben Sie die Optionen für den Metadaten-Zugriffsdienst-Prozess im folgenden Format ein:

```
... -o option_type.option_name=value
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Optionen für den Metadaten-Zugriffsdienst-Prozess beschrieben:

Option	Beschreibung
GeneralOptions.JVMOptions	Java Virtual Machine (JVM)-Befehlszeilenoptionen zum Ausführen von Java-basierten Programmen. Bei der Konfiguration von JVM-Optionen müssen Sie die Eigenschaften für den Java SDK-Klassenpfad, den Java SDK-Minimalspeicher und den Java SDK-Maximalspeicher festlegen.
HttpConfigurationOptions.KeyStoreFile	Pfad und Dateiname der Schlüsselspeicherdatei, die die Schlüssel und Zertifikate enthält, die zur Verwendung des HTTPS-Protokolls für den Metadaten-Zugriffsdienst erforderlich sind. Sie können eine Schlüsselspeicherdatei mit einem Keytool erstellen. Bei Keytool handelt es sich um ein Dienstprogramm, das private oder öffentliche Schlüsselpaare und zugeordnete Zertifikate in einer Schlüsselspeicherdatei erzeugt und speichert. Sie können das selbstsignierte Zertifikat nutzen oder ein Zertifikat verwenden, das von einer Zertifizierungsstelle signiert wurde.
HttpConfigurationOptions.KeyStorePassword	Passwort für die Schlüsselspeicherdatei.
HttpConfigurationOptions.MaxBacklogRequests	Anzahl der HTTP- oder HTTPS-Verbindungen, die in einer Warteschlange für diesen Metadaten-Zugriffsdienst-Prozess warten können. Standardwert ist 100.
HttpConfigurationOptions.MaxConcurrentRequests	Anzahl der HTTP- oder HTTPS-Verbindungen, die mit diesem Metadaten-Zugriffsdienst-Prozess hergestellt werden können. Der Minimalwert ist 4. Der Standardwert ist 200.
HttpConfigurationOptions.SSLProtocol	Zu verwendendes Secure Sockets Layer-Protokoll. Standardwert ist TLS.
HttpConfigurationOptions.TrustStoreFile	Pfad und Dateiname der Truststore-Datei, die Authentifizierungszertifikate enthält, die vom Metadaten-Zugriffsdienst als vertrauenswürdig eingestuft werden.
HttpConfigurationOptions.TrustStorePassword	Passwort für die Truststore-Datei.

# KAPITEL 24

## infacmd mi-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [abortRun, 864](#)
- [clearSamlConfig, 865](#)
- [createService, 866](#)
- [deploySpec, 870](#)
- [exportSpec, 871](#)
- [extendedRunStats, 872](#)
- [getSpecRunStats, 874](#)
- [listSpecRuns, 875](#)
- [listSpecs, 876](#)
- [restartMapping, 877](#)
- [runSpec, 879](#)
- [updateSamlConfig, 880](#)

### abortRun

Bricht die Erfassungszuordnungsjobs in einer Laufzeitinstanz einer Massenerfassungsspezifikation ab. Wenn Sie die Erfassungszuordnungsjobs abbrechen, bricht der Befehl die Zuordnungen ab, die die Erfassungsjobs für alle Quelltabellen durchführen, die ausgeführt oder in die Warteschlange gestellt werden. Die Zuordnungen für abgeschlossene Erfassungsaufträge werden nicht abgebrochen.

Zum Abbrechen der Erfassungszuordnungsjobs müssen Sie eine Laufzeit-ID angeben. Zum Auffinden der Ausführungs-ID für eine Ausführungsinstanz listen Sie die Ausführungsinstanzen der Spezifikation mithilfe von infacmd mi listSpecRuns auf.

Der Befehl „infacmd mi abortRun“ verwendet die folgende Syntax:

```
abortRun

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-ServiceName|-sn> service_name
```

```
<-runID|-rid> run_id
```

In der folgenden Tabelle werden die Optionen und Argumente für infacmd mi abortRun beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	password	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/ Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Optional. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung. Standardwert ist „Nativ“.
-ServiceName -sn	service_name	Erforderlich. Name des Massenerfassungsdiensts, der die Massenerfassungsspezifikation verwaltet.
-runID -rid	run_id	Erforderlich. Ausführungsidentifikationsnummer (Ausführungs-ID) der Ausführungsinstanz der Massenerfassungsspezifikation.  Zum Auffinden der Ausführungs-ID für eine Ausführungsinstanz listen Sie die Ausführungsinstanzen der Spezifikation mithilfe von infacmd mi listSpecRuns auf.

## clearSamlConfig

Löscht die SAML-Konfiguration des Massenerfassungsdiensts, um sie auf die Standardwerte zurückzusetzen.

Der Befehl „infacmd mi clearSamlConfig“ verwendet die folgende Syntax:

```
clearSamlConfig  
  
<-DomainName|-dn> domain_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-SecurityDomain|-sdn> security_domain]  
  
<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mi clearSamlConfig“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Optional. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Standardwert ist „Nativ“.
-ServiceName -sn	service_name	Erforderlich. Name des Massenerfassungsdiensts, der die Massenerfassungsspezifikation verwaltet.

## createService

Erstellt einen Massenerfassungsdienst. Beim Erstellen des Massenerfassungsdiensts müssen Sie einen Modellrepository-Dienst angeben. Der Massenerfassungsdienst ist standardmäßig deaktiviert. Verwenden Sie infacmd isp enableService, um den Massenerfassungsdienst zu aktivieren.

Der Befehl „infacmd mi createService“ verwendet die folgende Syntax:

```
createService
<-DomainName|-dn> domain_name
```

```

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-HttpPort|-http> http_port

[<-HttpsPort|-https> https_port]

[<-KeystoreFile|-kf> keystore_file_location]

[<-KeystorePassword|-kp> keystore_password]

<-LicenseName|-ln> license_name

[<-FolderPath|-fp> full_folder_path]

<-NodeName|-nn> node_name

<-RepositoryService|-rs> repository_service_name

[<-RepositoryUser|-ru> repository_user]

[<-RepositoryPassword|-rp> repository_password]

[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]

```

In der folgenden Tabelle werden die Optionen und Argumente für infacmd mi CreateService beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	password	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Optional. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Standardwert ist „Nativ“.
-Gateway -hp	gateway_host1:port gateway_host2:port	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Massenerfassungsdiensts.  Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 230 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten:  / * ? < > "
-HttpPort -http	http_port	Erforderlich, wenn Sie keinen HTTPS-Port angeben. Eindeutige HTTP-Portnummer, die für jeden Massenerfassungsdienstvorgang verwendet wird. Nachdem Sie den Dienst erstellt haben, können Sie für jeden Massenerfassungsdienstvorgang eine eigene Portnummer definieren.  Standardwert ist 9050. <b>Hinweis:</b> Sie können entweder einen HTTP- oder einen HTTPS-Port angeben.



Option	Argument	Beschreibung
-HttpsPort -https	https_port	Erforderlich, wenn Sie keinen HTTP-Port angeben. Eindeutige HTTPS-Portnummer, die für jeden Massenerfassungsdienstvorgang verwendet wird. Nachdem Sie den Dienst erstellt haben, können Sie für jeden Massenerfassungsdienstvorgang eine eigene Portnummer definieren. <b>Hinweis:</b> Sie können entweder einen HTTP- oder einen HTTPS-Port angeben.
-KeystoreFile -kf	keystore_file_location	Erforderlich, wenn Sie einen HTTPS-Port angeben. Pfad und Dateiname der Schlüsselspeicherdatei, die die Schlüssel und Zertifikate enthält, die zur Verwendung des HTTPS-Protokolls für den Massenerfassungsdienst erforderlich sind. Sie können eine Schlüsselspeicherdatei mit einem Keytool erstellen. Bei Keytool handelt es sich um ein Dienstprogramm, das private oder öffentliche Schlüsselpaare und zugeordnete Zertifikate in einer Schlüsselspeicherdatei erzeugt und speichert. Sie können das selbstsignierte Zertifikat nutzen oder ein Zertifikat verwenden, das von einer Zertifizierungsstelle signiert wurde.
-KeystorePassword -kp	keystore_password	Erforderlich, wenn Sie einen HTTPS-Port angeben. Passwort für die Schlüsselspeicherdatei.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz, die Sie dem Massenerfassungsdienst zuweisen möchten. Um Änderungen zu übernehmen, starten Sie den Massenerfassungsdienst neu.
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domännennamen) des Ordners, in dem der Massenerfassungsdienst erstellt werden soll. Folgendes Format ist erforderlich:  <i>/parent_folder/child_folder</i>  Standardwert ist die Domäne:  <i>/</i>
-NodeName -nn	node_name	Erforderlich. Knoten, auf dem der Massenerfassungsdienst ausgeführt wird.
-RepositoryService -rs	repository_service_name	Erforderlich. Modellrepository-Dienst, in dem die Metadaten für Massenerfassungsspezifikationen gespeichert werden.
-RepositoryUser -ru	repository_user	Optional. Benutzername zum Zugriff auf den Modellrepository-Dienst.

Option	Argument	Beschreibung
-RepositoryPassword -rp	repository_password	Erforderlich, wenn Sie den Benutzernamen angeben. Benutzerpasswort zum Zugriff auf den Modellrepository-Dienst.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Optional. Name der Sicherheitsdomäne, zu der der Benutzer des Modellrepositorys gehört.

## deploySpec

Stellt eine Massenerfassungsspezifikation bereit. Beim Bereitstellen der Spezifikation müssen Sie den Datenintegrationsdienst und die Hadoop-Verbindung angeben. Sie müssen eine Massenerfassungsspezifikation bereitstellen, bevor Sie sie ausführen können. Nach dem Bereitstellen der Spezifikation führen Sie sie mithilfe von infacmd mi runSpec aus.

Der Befehl „infacmd mi deploySpec“ verwendet die folgende Syntax:

```

deploySpec

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-ServiceName|-sn> service_name

<-DISServiceName|-dsn> dis_service_name

<-MISpecName|-spec> mi_spec_name

<-HadoopConnection|-hc> hadoop_connection

```

In der folgenden Tabelle werden die Optionen und Argumente für infacmd mi deploySpec beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Optional. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Standardwert ist „Nativ“.
-ServiceName -sn	service_name	Erforderlich. Name des Massenerfassungsdiensts, der die Massenerfassungsspezifikation verwaltet.
-DISServiceName -dis	data_integration_service	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Massenerfassungsspezifikation bereitgestellt werden soll.
-MISpecName -spec	mi_spec_name	Erforderlich. Name der Massenerfassungsspezifikation, die dem Datenintegrationsdienst bereitgestellt werden soll.
-HadoopConnection -hc	hadoop_connection	Erforderlich. Die vom Datenintegrationsdienst verwendete Hadoop-Verbindung zum Verlagern der Massenerfassungsspezifikation in die Hadoop-Umgebung.

## exportSpec

Exportiert die Massenerfassungsspezifikation in eine Anwendungsarchivdatei. Beim Exportieren der Spezifikation müssen Sie das Verzeichnis angeben, in dem die Datei gespeichert werden soll. Sie können die Anwendungsarchivdatei für einen Datenintegrationsdienst mithilfe des Befehls infacmd die DeployApplication bereitstellen.

Der Befehl „infacmd mi exportSpec“ verwendet die folgende Syntax:

```
exportSpec
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-ServiceName|-sn> service_name
<-MISpecName|-spec> mi_spec_name
<-Directory|-dir> dir_path
<-HadoopConnection|-hc> hadoop_connection
```

In der folgenden Tabelle werden die Optionen und Argumente für infacmd mit exportSpec beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	password	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Optional. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Standardwert ist „Nativ“.
-ServiceName -sn	service_name	Erforderlich. Name des Massenerfassungsdiensts, der die Massenerfassungsspezifikation verwaltet.
-MISpecName -spec	mi_spec_name	Erforderlich. Name der Massenerfassungsspezifikation, die exportiert werden soll.
-Directory -dir	dir_path	Erforderlich. Das Verzeichnis, in das die Anwendungsarchivdatei geschrieben werden soll.
-HadoopConnection -hc	hadoop_connection	Erforderlich. Die Hadoop-Verbindung, die der Datenintegrationsdienst zum Ausführen des Massenerfassungsauftrags verwendet, wenn Sie die Anwendungsarchivdatei importieren und die Anwendung ausführen.  Sie müssen die Hadoop-Verbindung angeben, da eine Hadoop-Verbindung für die Massenerfassungsspezifikation nicht beibehalten wird, während die Spezifikation im Modellrepository gespeichert wird.

## extendedRunStats

Ruft die Statistik über die erweiterte Erfassung für eine bestimmte Quelltable in einer bereitgestellten Massenerfassungsspezifikation ab. Zum Abrufen der erweiterten Statistiken müssen Sie die RunID der Massenerfassungsspezifikation, den Namen der Quelltable und den Zuordnungstyp angeben.

Die erweiterte Statistik meldet die Erfassungsstatistik der Tabellenzeilen, die aus der Quelle aufgenommen wurden, sowie die Erfassungsstatistik der Tabellenzeilen, die im Ziel aufgenommen wurden. Die Statistik

listet die Anzahl der Zeilen auf, die erfolgreich aufgenommen wurden, und die Anzahl der Zeilen, die Fehler enthalten.

Wenn die Ausführungsinstanz einen inkrementellen Ladevorgang verwendet, meldet die erweiterte Statistik ebenfalls den inkrementellen Schlüssel und den Startwert. Bei dem inkrementellen Schlüssel handelt es sich um den Namen der Spalte, die von der Spark-Engine zum Abrufen inkrementeller Daten in der Quelltable verwendet wurde. Der Startwert ist der Wert, der von der Spark-Engine zum Starten der Erfassung inkrementeller Daten verwendet wurde.

Der Befehl „infacmd mi extendedRunStats“ verwendet die folgende Syntax:

```
extendedRunStats

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-ServiceName|-sn> service_name

<-RunID|-rid> run_id

<-SourceName|-srcName> source_name

<-MappingTp|-mtp> mapping_type
```

In der folgenden Tabelle werden die Optionen und Argumente für infacmd mi extendedRunStats beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	password	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/ Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Optional. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung. Standardwert ist „Nativ“.
-ServiceName -sn	service_name	Erforderlich. Name des Massenerfassungsdiensts, der die mit dem Erfassungszuordnungsauftrag zugeordnete Massenerfassungsspezifikation verwaltet.

Option	Argument	Beschreibung
-RunID -rid	run_id	Erforderlich. Ausführungsidentifikationsnummer (Ausführungs-ID) der Ausführungsinstanz der Massenerfassungsspezifikation. Zum Auffinden der Ausführungs-ID für eine Ausführungsinstanz listen Sie die Ausführungsinstanzen der Spezifikation mithilfe von „infacmd mi listSpecRuns“ auf.
-SourceName -srcName	source_name	Erforderlich. Name der Quelltable in der Ausführungsinstanz der Massenerfassungsspezifikation. Zum Auffinden des Namens der Quelltable rufen Sie die Ausführungsstatistik der Erfassung mit „infacmd mi getSpecRunStats“ ab.
-MappingTp -mtp	mapping_type	Erforderlich. Der Zuordnungstyp entspricht der Laufzeit-Engine, die den Erfassungszuordnungsjob für die Quelltable ausführt. Zum Auffinden des Zuordnungstyps rufen Sie die Ausführungsstatistik der Erfassung mit „infacmd mi getSpecRunStats“ ab.

## getSpecRunStats

Ruft die ausführlichen Ausführungsstatistiken für eine bereitgestellte Massenerfassungsspezifikation ab. Zum Abrufen der Statistiken müssen Sie eine Ausführungs-ID angeben. Zum Auffinden der Ausführungs-ID für eine Ausführungsinstanz listen Sie die Ausführungsinstanzen der Spezifikation mithilfe von infacmd mi listSpecRuns auf.

Die detaillierte Ausführungsstatistik enthält die Auftrags-ID für jeden Erfassungszuordnungsauftrag in der bereitgestellten Massenerfassungsspezifikation, den Namen der Quelltabellen, die von den Zuordnungsaufträgen erfasst werden, die Startzeit, die Endzeit, die Laufzeit-Engine, die den Zuordnungsauftrag ausführt, und den Auftragsstatus. Die Auftrags-ID ist die ID des Erfassungszuordnungsauftrags, der die Quelltable erfasst. Der Status kann als abgeschlossen, fehlgeschlagen, abgebrochen, in Ausführung, in der Warteschlange oder unbekannt angegeben werden.

Der Befehl „infacmd mi getSpecRunStats“ verwendet die folgende Syntax:

```
getSpecRunStats
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-ServiceName|-sn> service_name
<-runID|-rid> run_id
```

In der folgenden Tabelle werden die Optionen und Argumente für infacmd mi getSpecRunStats beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	password	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/ Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Optional. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung. Standardwert ist „Nativ“.
-ServiceName -sn	service_name	Erforderlich. Name des Massenerfassungsdiensts, der die Massenerfassungsspezifikation verwaltet.
-runID -rid	run_id	Erforderlich. Ausführungsidentifikationsnummer (Ausführungs-ID) der Ausführungsinstanz der Massenerfassungsspezifikation.  Zum Auffinden der Ausführungs-ID für eine Ausführungsinstanz listen Sie die Ausführungsinstanzen der Spezifikation mithilfe von infacmd mi listSpecRuns auf.

## listSpecRuns

Listet die Ausführungsinstanzen einer bereitgestellten Massenerfassungsspezifikation auf. Jede Ausführungsinstanz wird durch eine Ausführungs-ID definiert. Beim Auflisten der Ausführungsinstanzen müssen Sie den Massenerfassungsdienst angeben.

Die detaillierte Ausführungsstatistik enthält die Ausführungs-ID für jede Spezifikationsausführungsinstanz, den Ladetyp, die Startzeit der Ausführungsinstanz, den Datenintegrationsdienst, in dem die Massenerfassungsspezifikation bereitgestellt wird, den Benutzer, der die Ausführung gestartet hat, und den Jobstatus jeder einzelnen Ausführungsinstanz. Der Status kann als abgeschlossen, fehlgeschlagen, abgebrochen, in Ausführung, in der Warteschlange oder unbekannt angegeben werden.

Der Befehl „infacmd mi listSpecRuns“ verwendet die folgende Syntax:

```
listSpecRuns
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
```

```

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-ServiceName|-sn> service_name

<-MISpecName|-spec> mi_spec_name

```

In der folgenden Tabelle werden die Optionen und Argumente für infacmd mi listSpecRuns beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	password	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/ Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Optional. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung. Standardwert ist „Nativ“.
-ServiceName -sn	service_name	Erforderlich. Name des Massenerfassungsdiensts, der die Massenerfassungsspezifikation verwaltet.
-MISpecName -spec	mi_spec_name	Erforderlich. Name der Massenerfassungsspezifikation.

## listSpecs

Listet die Massenerfassungsspezifikationen auf. Beim Auflisten von Spezifikationen müssen Sie den Massenerfassungsdienst angeben.

Der Befehl „infacmd mi listSpecs“ verwendet die folgende Syntax:

```

listSpecs

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

```



```
[<-SecurityDomain|-sdn> security_domain]
```

```
<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für infacmd mit listSpecs beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	password	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/ Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Optional. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung. Standardwert ist „Nativ“.
-ServiceName -sn	service_name	Erforderlich. Name des Massenerfassungsdiensts, der die Massenerfassungsspezifikationen verwaltet.

## restartMapping

Startet die Erfassungszuordnungsaufträge in einer Massenerfassungsspezifikation neu. Geben Sie die Liste der neu zu startenden Quelltabellen an. Sie müssen den Massenerfassungsdienst und die Ausführungs-ID der Ausführungsinstanz der Massenerfassungsspezifikation angeben. Sie können auch angeben, ob nur fehlgeschlagene Quelltabellen neu gestartet werden sollen.

Der Befehl „infacmd mit restartMapping“ verwendet die folgende Syntax:

```
restartMapping  
  
<-DomainName|-dn> domain_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-SecurityDomain|-sdn> security_domain]  
  
<-ServiceName|-sn> service_name
```

```
<-RunID|-rid> run_id
```

```
<-SourceList|-srcList> comma_separated_source_list
```

```
[<-OnlyFailed|-failed> true|false]
```

In der folgenden Tabelle werden die Optionen und Argumente für infacmd mi restartMapping beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	password	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Optional. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Standardwert ist „Nativ“.
-ServiceName -sn	service_name	Erforderlich. Name des Massenerfassungsdiensts, der die Erfassung der Quelltabellen verwaltet.
-runID -rid	run_id	Erforderlich. Ausführungs-ID der Ausführungsinstanz der Massenerfassungsspezifikation.
-SourceList -srcList	comma_separated_source_list	Erforderlich. Die Liste der Quelltabellen, die neu gestartet werden sollen. Trennen Sie die einzelnen Quelltabellen durch ein Komma.
-OnlyFailed -failed	true false	Optional. Geben Sie „true“ ein, um nur nicht erfasste Quelltabellen neu zu starten. Geben Sie „false“ ein, um alle Quelltabellen neu zu starten.

# runSpec

Führt eine Massenerfassungsspezifikation aus, die einem Datenintegrationsdienst bereitgestellt wird. Bevor Sie eine Spezifikation ausführen können, müssen Sie die Spezifikation mithilfe von infacmd mi deploySpec bereitstellen.

Der Befehl „infacmd mi runSpec“ verwendet die folgende Syntax:

```
runSpec  
  
<-DomainName|-dn> domain_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-SecurityDomain|-sdn> security_domain]  
  
<-ServiceName|-sn> service_name  
  
<-MISpecName|-spec> mi_spec_name  
  
[<-LoadType|-lt> load_type]  
  
<-DISServiceName|-dsn> dis_service_name  
  
[<-OperatingSystemProfile|-osp> operating_system_profile_name]
```

In der folgenden Tabelle werden die Optionen und Argumente für infacmd mi runSpec beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	password	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Optional. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Standardwert ist „Nativ“.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Massenerfassungsdiensts, der die Massenerfassungsspezifikation verwaltet.
-MISpecName -spec	mi_spec_name	Erforderlich. Name der Massenerfassungsspezifikation, die dem Datenintegrationsdienst bereitgestellt wird.
-LoadType -lt	load_type	Optional. Ladetyp zum Erfassen der Daten in der Massenerfassungsspezifikation. Verwenden Sie <b>Vollständig</b> oder <b>Inkrementell</b> . Standardwert ist <b>Vollständig</b> .  Wenn inkrementelles Laden in der Massenerfassungsspezifikation nicht aktiviert ist, können Sie inkrementelles Laden nicht zum Erfassen von Daten verwenden.
-DISServiceName -dis	data_integration_service	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Massenerfassungsspezifikation bereitgestellt wird.
-OperatingSystemProfile -osp	operating_system_profile_name	Optional. Name des Betriebssystemprofils, das für den Datenintegrationsdienst konfiguriert ist.

## updateSamlConfig

Aktualisiert die SAML-Konfiguration des Massenerfassungsdiensts. Sie können die Identitätsanbieter-URL, die Dienstanbieter-ID, die Zeitabweichungstoleranz und den Alias des Assertionssignierzertifikats konfigurieren.

Der Befehl „`infacmd mi updateSamlConfig`“ verwendet die folgende Syntax:

```
updateSamlConfig
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-ServiceName|-sn> service_name
[<-idpUrl|-iu> identity_provider_url]
[<-ServiceProviderId|-spid> service_provider_id]
[<-ClockSkewTolerance|-cst> clock_skew_tolerance_in_seconds]
[<-AssertionSigningCertificateAlias|-asca> idp_assertion_signing_certificate_alias]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mi updateSamlConfig“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Optional. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Standardwert ist „Nativ“.
-ServiceName -sn	service_name	Erforderlich. Name des Massenerfassungsdiensts, der die Massenerfassungsspezifikation verwaltet.
-idpUrl -iu	identity_provider_url	Optional. Geben Sie die URL des Identitäts-Providers für die Domäne an. Sie müssen die vollständige URL-Zeichenfolge angeben.
-ServiceProviderId -spid	service_provider_id	Optional. Der Vertrauensstellungsname der vertrauenswürdigen Partei oder die Kennung des Dienstbieters für die Domäne, wie im Identitätsanbieter definiert.  Wenn Sie „Informatica“ als Vertrauensstellungsname der vertrauenswürdigen Partei in AD FS angegeben haben, müssen Sie keinen Wert angeben.

Option	Argument	Beschreibung
-ClockSkewTolerance -cst	clock_skew_tolerance_i n_seconds	<p>Optional. Der zulässige zeitliche Unterschied zwischen der Systemuhr des Identitätsanbieter-Hosts und der Systemuhr auf dem Master-Gateway-Knoten.</p> <p>Die Lebensdauer der vom Identitäts-Provider ausgegebenen SAML-Token wird entsprechend der Systemuhr des Identitäts-Provider-Hosts festgelegt. Die Lebensdauer ist gültig, wenn die im Token festgelegte Startzeit oder Endzeit nicht mehr als die angegebene Anzahl an Sekunden von der Systemuhr auf dem Master-Gateway-Knoten abweicht.</p> <p>Die Werte müssen zwischen 0 und 600 Sekunden liegen. Standardwert ist 120 Sekunden.</p>
- AssertionSigningCertificate Alias -asca	idp_assertion_signing_ certificate_alias	<p>Optional. Der Aliasname, der beim Importieren des Assertionssignierzertifikats des Identitäts-Providers in die für die SAML-Authentifizierung verwendete Truststore-Datei angegeben wird.</p> <p>Importieren Sie zum Ändern des Aliasnamens das entsprechende Zertifikat in die Truststore-Datei auf allen Gateway-Knoten und starten Sie die Knoten dann neu.</p>

# KAPITEL 25

## infacmd mrs-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [BackupContents, 884](#)
- [CheckInObject, 886](#)
- [CreateContents, 888](#)
- [CreateFolder, 890](#)
- [CreateProject, 892](#)
- [CreateService, 894](#)
- [DeleteContents, 899](#)
- [DeleteFolder, 901](#)
- [DeleteProject, 903](#)
- [disableMappingValidationEnvironment, 905](#)
- [enableMappingValidationEnvironment, 909](#)
- [ListBackupFiles, 913](#)
- [ListCheckedOutObjects, 915](#)
- [listFolders, 917](#)
- [ListLockedObjects, 919](#)
- [listMappingEngines, 921](#)
- [listPermissionOnProject, 923](#)
- [ListProjects, 925](#)
- [ListServiceOptions, 927](#)
- [ListServiceProcessOptions, 929](#)
- [ManageGroupPermissionOnProject, 931](#)
- [ManageUserPermissionOnProject, 933](#)
- [PopulateVCS, 935](#)
- [ReassignCheckedOutObject, 936](#)
- [rebuildDependencyGraph, 938](#)
- [RenameFolder, 940](#)
- [replaceMappingHadoopRuntimeConnections, 942](#)
- [RestoreContents, 944](#)
- [UndoCheckout, 946](#)
- [setMappingExecutionEnvironment, 948](#)

- [UndoCheckout, 950](#)
- [UnlockObject, 952](#)
- [UpdateServiceOptions, 954](#)
- [UpdateServiceProcessOptions, 961](#)
- [UpdateStatistics, 963](#)
- [UpgradeContents, 965](#)
- [UpgradeExportedObjects, 967](#)

## BackupContents

Sichert den Inhalt des Modellrepository in einer Datei. Wenn der Repository-Inhalt nicht vorhanden ist, schlägt der Befehl fehl.

Um sicherzustellen, dass eine konsistente Backup-Datei erstellt wird, blockiert die Backup-Operation alle anderen Repository-Operationen so lange, bis das Backup abgeschlossen ist.

Der Befehl „`infacmd mrs BackupContents`“ verwendet die folgende Syntax:

```
BackupContents
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-OutputFileName|-of> output_file_name
[<-OverwriteFile|-ow> overwrite_file]
[<-Description|-ds> description]
[<-BackupSearchIndices|-bsi> backup_search_index]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```



In der folgenden Tabelle werden Optionen und Argumente für „infacmd mrs BackupContents“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Dienst.
OutputFileName -of	output_file_name	Erforderlich. Name der Backup-Datei.
OverwriteFile -ow	overwrite_file	Sie müssen diese Option einbeziehen, um eine Backup-Datei mit demselben Namen zu überschreiben.

Option	Argument	Beschreibung
Beschreibung -ds	Beschreibung	Beschreibung der Backup-Datei. Wenn die Beschreibung Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie die Beschreibung in Anführungszeichen ein.
-BackupSearchIndices -bsi	-	Optional. Setzen Sie den Wert auf TRUE, um den Suchindex in der Backup-Datei zu speichern und die zum Wiederherstellen der Datei benötigte Zeit zu verringern. Setzen Sie den Wert auf FALSE, um den Suchindex nicht in der Backup-Datei zu speichern. Wenn Sie die Datei wiederherstellen, erstellt der Modellrepository-Dienst den Suchindex neu. Standardwert ist „true“.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## CheckInObject

Checkt ein einzelnes ausgechecktes Objekt ein. Das Objekt wird in das Modellrepository eingechekkt.

Der infacmd mrs CheckInObject-Befehl verwendet die folgende Syntax:

```
infacmd mrs checkInObject
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ObjectPathandName|-opn> object_path_and_name
[<-Description|-ds> description]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs CheckInObject“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ObjectPathAndName -opn	MRS_object_path	Erforderlich. Pfad zum Modellrepository-Objekt, einschließlich Objektname. Setzen Sie den Pfad in doppelte Anführungszeichen. Verwenden Sie folgende Syntax: "ProjectName/FolderName/.../SubFolder_Name/{ObjectName ProjectName/ObjectName}"
-Description -ds	Beschreibung	Optional. Sie können diesen Parameter für die Eincheckbeschreibung oder für Eincheckkommentare verwenden.

## CreateContents

Erstellt Repository-Inhalt für ein Modellrepository. Der Befehl schlägt fehl, wenn der Inhalt für das Modellrepository vorhanden ist.

Der Befehl „infacmd mrs CreateContents“ verwendet die folgende Syntax:

```
CreateContents
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs CreateContents“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## CreateFolder

Erstellt einen Ordner in einem Projekt in einem Modellrepository.

Der infacmd mrs CreateFolder-Befehl verwendet die folgende Syntax:

```
infacmd mrs createFolder
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
<-Path|-p> folder_path_and_name
[<-CreatePath|-cp> true|false]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs CreateFolder“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.

Option	Argument	Beschreibung
-ProjectName -pn	project_name	Erforderlich. Name des Projekts, in dem der Ordner erstellt werden soll.  Beim Projektnamen wird die Groß-/Kleinschreibung nicht beachtet. Der Projektname darf nicht mehr als 128 Zeichen umfassen. Der Projektname darf nicht mit einer Zahl beginnen und kann alphanumerische Zeichen und die folgenden Zeichen enthalten:  @ # _
-Path -p	folder_path_and_name	Erforderlich. Pfad und Name des zu erstellenden Ordners. Der Pfadname muss mit einem Schrägstrich (/) beginnen.
-CreatePath -cp	true false	Optional. Wenn TRUE, wird der Ordner im angegebenen Pfad erstellt. Standardwert ist FALSE.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## CreateProject

Erstellt ein Projekt in einem Modellrepository.

Der Befehl „infacmd mrs CreateProject“ verwendet die folgende Syntax:

```
infacmd mrs createProject
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```



In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs CreateProject“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.

Option	Argument	Beschreibung
-ProjectName -pn	project_name	Erforderlich. Name des zu erstellenden Projekts. Beim Projektname wird die Groß-/Kleinschreibung nicht beachtet. Der Projektname darf nicht mehr als 128 Zeichen umfassen. Der Projektname darf nicht mit einer Zahl beginnen und kann alphanumerische Zeichen und die folgenden Zeichen enthalten:  @ # _
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## CreateService

Erstellt einen Modellrepository-Dienst. Bevor Sie den Modellrepository-Dienst erstellen, müssen Sie zum Speichern von Repository-Tabellen eine Datenbank anlegen. Verwenden Sie den Datenbank-Client zum Erstellen der Datenbank.

Jedes Modellrepository muss die folgenden Datenbankanforderungen erfüllen:

- Das Modellrepository muss ein eindeutiges Schema aufweisen. Es ist nicht möglich, dass zwei Modellrepositories oder ein Modellrepository und die Domänenkonfigurationsdatenbank dasselbe Schema verwenden.
- Das Modellrepository muss einen eindeutigen Repository-Datenbanknamen aufweisen.

Der Befehl „`infacmd mrs CreateService`“ verwendet die folgende Syntax:

```
CreateService
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-DbUser|-du> db_user
<-DbPassword|-dp> db_password
<-DbUrl|-dl> db_url
[<-DbDriver|-dr> db_driver]
[<-DbDialect|-dd> db_dialect]
```

```
[<-SearchIndexRoot|-si> search_index_root]

[<-DbType|-dt> db_type (ORACLE, DB2, SQLSERVER, OR POSTGRESQL)]

[<-DbSchema|-ds> db_schema (Used only for Microsoft SQL Server and
PostgreSQL databases)]

[<-DbTablespace|-db> db_tablespace (used for IBM DB2 only)]

[<-SecureJDBCParameters|-sjdbc> secure_jdbc_parameters]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-FolderPath|-fp> full_folder_path]

[<-BackupNodes|-bn> nodename1,nodename2,...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs CreateService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
NodeName -nn	node_name	Erforderlich. Knoten, auf dem der Modellrepository-Dienst ausgeführt werden soll.
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
-DbUser -du	db_user	Erforderlich. Konto für die Repository-Datenbank. Richten Sie dieses Konto mithilfe des Datenbank-Clients ein.
-DbPassword -dp	db_password	Erforderlich. Passwort der Repository-Datenbank für den Datenbankbenutzer.

Option	Argument	Beschreibung
-DbUrl -dl	db_url	<p>Erforderlich.</p> <p>Die JDBC-Verbindungszeichenfolge für die Verbindung mit der Modellrepository-Datenbank. Verwenden Sie die folgende Syntax für jede unterstützte Datenbank:</p> <ul style="list-style-type: none"> <li>- <b>IBM Db2.</b> "jdbc:informatica:db2://&lt;host name&gt;:&lt;port number&gt;;DatabaseName=&lt;database name&gt;;BatchPerformanceWorkaround=true;DynamicSections=3000"</li> <li>- <b>Microsoft SQL Server, der die Standardinstanz verwendet.</b> "jdbc:informatica:sqlserver://&lt;host name&gt;:&lt;port number&gt;;DatabaseName=&lt;database name&gt;;SnapshotSerializable=true"</li> <li>- <b>Microsoft SQL Server, der eine benannte Instanz verwendet.</b> "jdbc:informatica:sqlserver://&lt;host name&gt;\&lt;named instance name&gt;;DatabaseName=&lt;database name&gt;;SnapshotSerializable=true"</li> <li>- <b>Microsoft SQL Server, der die Standardinstanz mit Windows NT-Anmeldedaten verwendet.</b> "jdbc:informatica:sqlserver://&lt;host name&gt;:&lt;port number&gt;;DatabaseName=&lt;database name&gt;;SnapshotSerializable=true;authenticationMethod=NTLM"</li> <li>- <b>Microsoft SQL Server, der die benannte Instanz mit Windows NT-Anmeldedaten verwendet.</b> "jdbc:informatica:sqlserver://&lt;host name&gt;\&lt;named instance name&gt;;DatabaseName=&lt;database name&gt;;SnapshotSerializable=true;authenticationMethod=NTLM"</li> <li>- <b>Azure SQL Server.</b> "jdbc:informatica:sqlserver://&lt;host name&gt;:&lt;port number&gt;;DatabaseName=&lt;database name&gt;;SnapshotSerializable=true;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.&lt;hostnamein certificate&gt;;ValidateServerCertificate=true"</li> <li>- <b>Azure SQL Database mit Active Directory-Authentifizierung.</b> "jdbc:informatica:sqlserver://&lt;host_name&gt;:&lt;port_number&gt;;database=&lt;database_name&gt;;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostnameInCertificate=*.database.windows.net;loginTimeout=&lt;seconds&gt;"</li> <li>- <b>Oracle.</b> "jdbc:informatica:oracle://&lt;host name&gt;:&lt;port number&gt;;SID=&lt;database name&gt;;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true"</li> </ul>

Option	Argument	Beschreibung
		<p>Zum Herstellen einer Verbindung zu Oracle mithilfe des Oracle-Verbindungsmanagers verwenden Sie folgende Verbindungszeichenfolge:</p> <pre>" jdbc:Informatica:oracle:TNSNamesFile=&lt;fully qualified path to the tnsnames.ora file&gt;;TNSServerName=&lt;TNS server name&gt;; "</pre> <p>- PostgreSQL. "jdbc:informatica:postgresql://&lt;host name&gt;:&lt;port number&gt;;DatabaseName= "</p>
-DbDriver -dr	db_driver	Optional. Der Data Direct-Treiber zum Herstellen einer Verbindung zur Datenbank. Beispiel: com.informatica.jdbc.oracle.OracleDriver
-DbDialect -dd	db_dialect	Optional. Der SQL-Dialekt für eine bestimmte Datenbank. Der Dialekt ordnet Objekte zu Datenbankobjekten hinzu. Beispiel: org.hibernate.dialect.Oracle9Dialect
-SearchIndexRoot -si	search_index_root	Optional. Ändert das Verzeichnis für den Suchindex. Geben Sie den vollständigen Pfad zum Verzeichnis ein. Standardmäßig wird das Informatica-Installationsverzeichnis verwendet.
-DbType -dt	db_type	Optional. Werte sind „Oracle“, „SQL Server“, „DB2“ oder „PostgreSQL“.
-DbSchema -ds	db_schema	Optional. Der Schemaname für eine Microsoft SQL Server-Datenbank oder eine PostgreSQL-Datenbank.
-DbTablespace -dt	db_tablespace	Nur für eine DB2-Datenbank erforderlich. Beim Konfigurieren eines Tablespace-Namens erstellt der Modellrepository-Dienst alle Repository-Tabellen im selben Tablespace. Sie können im Tablespace-Namen keine Leerzeichen verwenden.
[<-SecureJDBCParameters>-sjdbcp> secure_jdbc_parameters]	Sichere JDBC-Parameter	<p>Wenn die Modellrepository-Datenbank mittels SSL-Protokoll gesichert wird, müssen Sie die sicheren Datenbankparameter eingeben.</p> <p>Geben Sie die Parameter als name=value-Paare, getrennt durch ein Semikolon (;) ein. Beispiel: param1=value1;param2=value2</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad ohne Domännennamen zu dem Ordner, in dem Sie den Dienst erstellen möchten. Folgendes Format ist erforderlich:  <i>/parent_folder/child_folder</i> Standardwert ist „/“ (die Domäne).
-BackupNodes -bn	nodename1,nodename2,...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Backup-Knoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.

## DeleteContents

Löscht den Inhalt des Modellrepository. Der Befehl schlägt fehl, wenn der Inhalt für das Modellrepository nicht vorhanden ist.

Der Befehl „infacmd mrs DeleteContents“ verwendet die folgende Syntax:

```

DeleteContents

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs DeleteContents“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.



Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## DeleteFolder

Löscht einen Ordner aus einem Projekt in einem Modellrepository.

Zum Löschen eines Ordners, der Objekte enthält, legen Sie die Option -ForceDelete auf TRUE fest.

Der infacmd mrs DeleteFolder-Befehl verwendet die folgende Syntax:

```
infacmd mrs deleteFolder
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
<-Path|-p> folder_path_and_name
[<-ForceDelete|-f> true|false]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs DeleteFolder“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
-ProjectName -pn	project_name	Erforderlich. Name des Projekts, das den Ordner enthält.
-Path -p	folder_path_and_name	Erforderlich. Pfad und Name des zu löschenden Ordners. Pfad muss mit einem Schrägstrich (/) beginnen.

Option	Argument	Beschreibung
-ForceDelete -f	true false	Optional. Wenn TRUE, wird ein Ordner mit Objekten gelöscht. Standardwert ist „false“.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## DeleteProject

Löscht ein Projekt in einem Modellrepository.

Legen Sie die Option -ForceDelete auf TRUE fest, um ein Projekt mit Ordnern und Objekten zu löschen.

Der infacmd mrs DeleteProject-Befehl verwendet die folgende Syntax:

```
infacmd mrs deleteProject
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
[<-ForceDelete|-f> true|false]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs DeleteProject“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
-ProjectName -pn	project_name	Erforderlich. Name des zu löschenden Projekts.

Option	Argument	Beschreibung
-ForceDelete -f	true false	Optional. Wenn TRUE, wird ein Projekt mit Ordnern und Objekten gelöscht. Standardwert ist „false“.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## disableMappingValidationEnvironment

Deaktiviert die ausgewählte Validierungsumgebung für Zuordnungen, die Sie über das Developer Tool ausführen.

Verwenden Sie den ValidationEnvironment-Parameter, um eine Validierungsumgebung für ein Mapping zu deaktivieren. Wiederholen Sie den Befehl für jede Umgebung, die Sie entfernen möchten.

Verwenden Sie Filter, um ein oder mehrere Mappings in einem Projekt zu aktualisieren. Wenn Sie Filter einschließen, aktualisiert der Befehl alle Mappings, die nicht im Datenintegrationsdienst bereitgestellt werden. Damit ein Mapping geändert werden kann, muss es allen festgelegten Filtern entsprechen.

Der Befehl infacmd mrs disableMappingValidationEnvironment verwendet die folgende Syntax:

```
disableMappingValidationEnvironment
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ProjectName|-pn> project_name]
[<-MappingNamesFilter|-mnf> mapping_names]
[<-ExecutionEnvironmentFilter|-eef> execution_environment_name]
[<-ExecutionEnvironmentParameterNameFilter|-pnf> parameter_name]
[<-ExecutionEnvironmentParameterDefaultValueFilter|-pdvf> parameter default value]
<-ValidationEnvironment|-ve> validation_environment_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente von disableMappingValidationEnvironment beschrieben:

Option	Argument	Beschreibung
DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>

Option	Argument	Beschreibung
UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
Passwort -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
ProjectName -pn	project_name	<p>Optional. Name des Projekts, das das Mapping enthält. Wenn Sie keinen Projektnamen angeben, aktualisiert der Befehl alle Projekte im Modellrepository.</p> <p>Sie können jeweils nur ein Projekt angeben.</p>
MappingNamesFilter -mnf	mapping_names	<p>Optional. Die Namen der Mappings, für die Sie die Validierungsumgebung deaktivieren möchten. Trennen Sie die Namen der Mappings durch Kommas.</p> <p>Standardmäßig werden alle Mappings im Modellrepository berücksichtigt.</p>

Option	Argument	Beschreibung
ExecutionEnvironmentFilter -eef	execution_environment_name	Optional. Geben Sie die Ausführungsumgebung für die zu entfernende Validierungsumgebung an. Sie können entweder „Nativ“, „Hadoop“ oder „Databricks“ eingeben.  Standardmäßig wird die Validierungsumgebung für alle Engines auf Basis anderer Filterkriterien geändert.
ValidationEnvironment -ve	validation_environment_name	Erforderlich. Name der Validierungsumgebung, die aus einem Mapping entfernt werden soll. Sie können einen der folgenden Werte eingeben: <ul style="list-style-type: none"> <li>- native</li> <li>- blaze</li> <li>- spark</li> <li>- spark-databricks</li> </ul> Führen Sie den Befehl für jede zu entfernende Validierungsumgebung aus.
ExecutionEnvironmentParameterNameFilter -pnf	name_of_parameter	Optional. Wählt nur Zuordnungen aus, deren Parametername mit diesem Wert übereinstimmt.  Beispiel: infacmd.sh mrs enableValidationEnvironment -pnf MyParam -ve Databricks
ExecutionEnvironmentParameterDefaultValueFilter -pdvf	parameter_default_value	Optional. Wählt nur Zuordnungen aus, deren standardmäßiger Parametername mit diesem Wert übereinstimmt.  Beispiel: infacmd.sh mrs enableValidationEnvironment -pdvf Hadoop -ve Databricks
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.



# enableMappingValidationEnvironment

Aktiviert eine Validierungsumgebung für Zuordnungen, die Sie über das Developer Tool ausführen. In den Eigenschaften der Validierungsumgebung für Zuordnungen werden die Engines angegeben, auf denen die Zuordnung zur Ausführung validiert wird.

Verwenden Sie den ValidationEnvironment-Parameter, um eine Validierungsumgebung für ein Mapping anzugeben. Wiederholen Sie den Befehl und geben Sie eine andere Validierungsumgebung an, um eine zusätzliche Validierungsumgebung für das Mapping zu aktivieren.

Verwenden Sie Filter, um ein oder mehrere Mappings in einem Projekt zu aktualisieren. Wenn Sie keine Filter einschließen, aktualisiert der Befehl alle Mappings, die nicht im Datenintegrationsdienst bereitgestellt werden. Damit ein Mapping geändert werden kann, muss es allen festgelegten Filtern entsprechen.

Der Befehl `infacmd mrs enableMappingValidationEnvironment` verwendet die folgende Syntax:

```
enableMappingValidationEnvironment
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ProjectName|-pn> project_name]
[<-ConnectionName|-cn> connection_name]
[<-MappingNamesFilter|-mnf> mapping_names]
[<-ExecutionEnvironmentFilter|-eef> execution_environment_name]
[<-ExecutionEnvironmentParameterNameFilter|-pnf> parameter_name]
[<-ExecutionEnvironmentParameterDefaultValueFilter|-pdvf> parameter default value]
<-ValidationEnvironment|-ve> validation_environment_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente von enableMappingValidationEnvironment beschrieben:

Option	Argument	Beschreibung
DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>

Option	Argument	Beschreibung
UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
Passwort -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
ProjectName -pn	project_name	<p>Optional. Name des Projekts, das das Mapping enthält. Wenn Sie keinen Projektnamen angeben, aktualisiert der Befehl alle Projekte im Modellrepository.</p> <p>Sie können jeweils nur ein Projekt angeben.</p>

Option	Argument	Beschreibung
ConnectionName -cn	connection_name	<p>Name der Verbindung für die zu verwendende Mapping-Validierungsumgebung. Die Verbindung überschreibt eine vorhandene Verbindung oder einen Verbindungsparameter, der für die Umgebung festgelegt wurde.</p> <p>Erforderlich, um die native oder nicht-native Umgebung zu aktivieren, wenn in der angegebenen Zuordnung keine Verbindung vorhanden ist. Optional, um die native Umgebung zu aktivieren, oder wenn bereits eine Verbindung vorhanden ist.</p>
MappingNamesFilter -mnf	mapping_names	<p>Optional. Die Namen der Mappings, für die Sie die Validierungsumgebung aktivieren möchten. Trennen Sie die Namen der Mappings durch Kommas.</p> <p>Standardmäßig werden alle Mappings im Modellrepository berücksichtigt.</p>
ExecutionEnvironmentFilter -eef	execution_environment_name	<p>Optional. Geben Sie die Ausführungsumgebung an, nach der gefiltert werden soll. Sie können entweder „Nativ“, „Hadoop“ oder „Databricks“ eingeben.</p> <p>Standardmäßig wird die Validierungsumgebung für alle Engines auf Basis anderer Filterkriterien geändert.</p>
ValidationEnvironment -ve	validation_environment_name	<p>Erforderlich. Name der Validierungsumgebung, die für ein Mapping aktiviert werden soll. Sie können einen der folgenden Werte eingeben:</p> <ul style="list-style-type: none"> <li>- native</li> <li>- blaze</li> <li>- spark</li> <li>- spark-databricks</li> </ul> <p>Führen Sie den Befehl für jede zu aktivierende Validierungsumgebung aus.</p>
ExecutionEnvironmentParameterNameFilter -pnf	name_of_parameter	<p>Optional. Wählt nur Zuordnungen aus, deren Parametername mit diesem Wert übereinstimmt.</p> <p>Beispiel: <code>infacmd.sh mrs enableValidationEnvironment -pnf MyParam -ve Databricks</code></p>

Option	Argument	Beschreibung
ExecutionEnvironmentParameterDefaultValueFilter -pdvf	parameter_default_value	Optional. Wählt nur Zuordnungen aus, deren standardmäßiger Parametername mit diesem Wert übereinstimmt.  Beispiel: infacmd.sh mrs enableValidationEnvironment -pdvf Hadoop -ve Databricks
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

## ListBackupFiles

Listet Dateien im Backup-Ordner auf.

Der Befehl „infacmd mrs ListBackupFiles“ verwendet die folgende Syntax:

```
ListBackupFiles
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs ListBackupFiles“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Dienst.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## ListCheckedOutObjects

Zeigt eine Liste von Objekten an, die von einem Benutzer ausgecheckt wurden. Führen Sie diesen Befehl für ein Repository aus, das in ein Versionsverwaltungssystem integriert ist.

Der Befehl „infacmd mrs listCheckedOutObjects“ verwendet die folgende Syntax:

```
infacmd mrs listCheckedOutObjects
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-ByUser|-bu> by_user_name]
[<-ByUserSecurityDomain|-bsd> by_user_security_domain]
[<-ObjectType|-ot> object_type]
[<-ByObjectPathandName|-bopn> object_path_and_name]
[<-objectName|-objn> object_name]
[<-operationType|-otype> operation_type]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs listCheckedOutObjects“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.



Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ByUser -bu	checkedout_by_user	Optional. Benutzerkonto, von dem Objekte im Modellrepository ausgecheckt wurden.
-ObjectType -ot	object_type	Optional. Typ des zu suchenden Objekts. Beispiel: Mapping.
-ByObjectPathandName -bopn	object_path_and_name	Optional. Pfad und Name des zu suchenden Objekts.
-ObjectName -objn	object_name	Optional. Name des zu suchenden Objekts.
-LastOperationType -optype	operation_type	Optional. Typ des zu suchenden Vorgangs. Geben Sie einen der folgenden Werte ein: - ADD_OP - EDIT_OP - MOVE_OP - DELETE_OP

## listFolders

Listet die Namen aller Ordner im angegebenen Projektordnerpfad auf.

Verwenden Sie die Option -Path, um alle Ordner in einem Projekt oder alle in einem Unterordner enthaltenen Ordner aufzulisten. Verwenden Sie einen Schrägstrich (/) zur Angabe der obersten Ebene eines Projekts.

Der folgende Befehl listet beispielsweise alle Ordner in /MRS\_1/Projekt\_A/ auf:

```
infacmd mrs listFolders ... -sn MRS_1 -pn Project_A -p /
```

Enthält Projekt\_A Ordner\_1 und Ordner\_2, listet der folgende Befehl alle Unterordner in Ordner\_1 auf:

```
infacmd mrs listFolders ... -sn MRS_1 -pn Project_A -p /Folder_1/
```

Der infacmd mrs ListFolders-Befehl verwendet die folgende Syntax:

```
infacmd mrs listFolders
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
<-Path|-p> path
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs ListFolders“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.

Option	Argument	Beschreibung
-ProjectName -pn	project_name	Erforderlich. Name des Projekts, für das Sie die Ordner auflisten möchten.  Beim Projektnamen wird die Groß-/Kleinschreibung nicht beachtet. Der Projektname darf nicht mehr als 128 Zeichen umfassen. Der Projektname darf nicht mit einer Zahl beginnen und kann alphanumerische Zeichen und die folgenden Zeichen enthalten:  @ # _
-Path -p	path	Erforderlich. Pfad zu dem übergeordneten Ordner, in dem Ordnerinhalte aufgelistet werden sollen.  Der Pfad muss mit einem Schrägstrich (/) beginnen. Bei diesem Namen wird die Groß-/Kleinschreibung nicht beachtet.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## ListLockedObjects

Zeigt eine Liste von Objekten an, die von einem Benutzer gesperrt wurden. Führen Sie diesen Befehl für ein Repository aus, das nicht in ein Versionsverwaltungssystem integriert ist.

**Hinweis:** Wenn Sie diesen Befehl für ein versioniertes Repository ausführen, schlägt der Befehl fehl.

Der Befehl „infacmd mrs listLockedObjects“ verwendet die folgende Syntax:

```
infacmd mrs listLockedObjects
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-ByUser|-bu> user_name]
[<-ByUserSecurityDomain|-bsd> by_user_security_domain]
[<-ObjectType|-ot> object_type]
[<-ByObjectPathandName|-bopn> object_path_and_name]
[<-objectName|-objn> object_name]
[<-lastOperationType|-otype> operation_type]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs listLockedObjects“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ByUser -bu	locked_by_user	Optional. Benutzerkonto, das Besitzer der Sperre für Objekte im Modellrepository ist. Standard sind von allen Benutzern gesperrte Objekte.
-ObjectType -ot	object_type	Optional. Typ des zu suchenden Objekts. Sie können den Befehl für einen Objekttyp ausführen. Wenn Sie den Parameter nicht angeben, wird der Befehl für alle Objekttypen ausgeführt.
-ByObjectPathAndName -bopn	object_path_and_name	Optional. Modellrepository-Pfad und -Name des zu suchenden Objekts.
-ObjectName -objn	object_name	Optional. Name des zu suchenden Objekts.
-LastOperationType -optype	operation_type	Optional. Typ des zu suchenden Vorgangs. Geben Sie einen der folgenden Werte ein: - ADD_OP - EDIT_OP - MOVE_OP - DELETE_OP

## listMappingEngines

Listet die Laufzeit-Engines der Zuordnungen auf, die über das Developer Tool ausgeführt werden. Sie können die Ergebnisse nach Projekt, Validierungsumgebung und Laufzeitumgebung sowie nach Parametern für die Laufzeitumgebung filtern.

Der Befehl „infacmd mrs listMappingEngines“ verwendet die folgende Syntax:

```
listMappingEngines
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ProjectNames|-pn>] project_name
[-ValidationEnvironmentFilter|-vef] validation_environment_name
```

```
[<-ExecutionEnvironmentFilter|-eef> execution_environment_name]
```

```
[<-ExecutionEnvironmentParameterNameFilter|-pnf> execution_environment_parameter_name]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für `infacmd mts listMappingEngines` beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.

Option	Argument	Beschreibung
ProjectName -pn	project_name	Optional. Name des Projekts, das die Zuordnung enthält. Wenn Sie keinen Projektnamen angeben, listet der Befehl alle Projekte und die Zuordnungen innerhalb der Projekte auf. Sie können jeweils nur ein Projekt angeben.
ValidationEnvironmentFilter -ve	validation_environment_name	Optional. Name der Validierungsumgebung, für die Sie die Liste der Zuordnungen anzeigen möchten. Wählen Sie einen der folgenden Werte aus: - native - blaze - spark - spark-databricks Führen Sie den Befehl für jede Validierungsumgebung aus, um die Zuordnungen aufzulisten.
ExecutionEnvironmentFilter -eef	execution_environment_name	Optional. Geben Sie die Laufzeitumgebung an, nach der Sie die Zuordnungen filtern möchten. Wählen Sie entweder „Nativ“, „Hadoop“ oder „Databricks“ aus. Wenn Sie beispielsweise „Nativ“ angeben, listet der Befehl die Zuordnungen auf, die zur Ausführung im Datenintegrationsdienst konfiguriert sind.
ExecutionEnvironmentParameterNameFilter -pnf	execution_environment_parameter_name	Optional. Geben Sie den Namen des Parameters für die Parametrisierung von Laufzeitumgebung und -filter an. Sie können die Laufzeitumgebungen in der Parameterdatei zusammen mit einer Variablen parametrisieren und die Variable im infacmd-Befehl verwenden.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## listPermissionOnProject

Listet alle Berechtigungen in verschiedenen Projekten für Gruppen und Benutzer auf. Trennen Sie die einzelnen Projektnamen durch Kommas. Sie benötigen eine Leseberechtigung für das Projekt, um die Liste der Berechtigungen für die Gruppen und Benutzer anzeigen zu können.

Der Befehl „infacmd mrs listPermissionOnProject“ verwendet die folgende Syntax:

```
listPermissionOnProject
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
```

```

<-Password|-pd> password

<-ServiceName|-sn> service_name

<-ProjectNames|-pn> project_name_list

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

```

In der folgenden Tabelle werden die Optionen und Argumente für `infacmd mrs listPermissionOnProject` beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.



Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
-ProjectNames -pn	project_name_list	Erforderlich. Namen der Projekte, für die Sie die Berechtigungen für Benutzer und Gruppen auflisten möchten.  Bei Projektnamen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Trennen Sie die einzelnen Projektnamen durch Kommas.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## ListProjects

Listet Projekte im Modellrepository auf. Der Befehl schlägt fehl, wenn das Modellrepository keinen Repository-Inhalt aufweist.

Der Befehl „infacmd mrs ListProjects“ verwendet die folgende Syntax:

```
ListProjects
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs ListProjects“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Dienst.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## ListServiceOptions

Listet Optionen für den Modellrepository-Dienst auf.

Der Befehl „infacmd mrs ListServiceOptions“ verwendet die folgende Syntax:

```
ListServiceOptions
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs ListServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Dienst.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## ListServiceProcessOptions

Listet Dienstprozess-Optionen für den Modellrepository-Dienst auf.

Der Befehl „infacmd mrs ListServiceProcessOptions“ verwendet die folgende Syntax:

```
ListServiceOptions
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs ListServiceProcessOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
NodeName -nn	node_name	Erforderlich. Knotenname, für den die Dienstprozessoptionen aufgelistet werden sollen.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

# ManageGroupPermissionOnProject

Manages permissions on multiple projects for a group.

The infacmd mrs manageGroupPermissionOnProject command uses the following syntax:

```
infacmd mrs manageGroupPermissionOnProject
<-DomainName|-dn> domain_name
[<-SecurityDomain |-sdn> security_domain]
[<-recipientSecurityDomain|-rdn> recipient_security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectNames|-pn> project_name_list
<-Permission|-pm> permission_name
<-RecipientName|-rn> recipient_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs ManageGroupPermissionOnProject options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.  If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-recipientSecurityDomain -rdn	recipient_security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the recipient group belongs.  To set the recipient security domain, refer to the same guidelines that you use to set the security domain for the authorizing user.

Option	Argument	Description
-UserName -un	user_name	<p>Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.</p> <p>Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.</p>
-Password -pd	password	<p>Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.</p>
-ServiceName -sn	service_name	<p>Required. Model Repository Service name.</p>
-ProjectNames -pn	project_name_list	<p>Required. Names of the projects for which you want to allow or revoke permissions.</p> <p>The project names are not case sensitive.</p> <p>Separate multiple project names with a comma.</p>
-Permission -pm	permission_name	<p>Required. The permissions that you want to allow or revoke from the recipient group.</p> <p>Enter the permission in double quotes and use a backslash ( \ ) as the escape character.</p> <p>The following arguments are valid:</p> <p>+r, +w, +g, -r, -w, -g</p> <p>Use these arguments to allow or revoke read, write, and grant permissions.</p> <p>For example, a valid argument to revoke read permissions and allow write permissions is \ "-r+w\".</p>
-RecipientName -rn	recipient_name	<p>Required. The name of the recipient group for which you want to manage permissions.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.</p>



# ManageUserPermissionOnProject

Manages permissions on multiple projects for a user.

The infacmd mrs manageUserPermissionOnProject command uses the following syntax:

```
infacmd mrs manageUserPermissionOnProject
<-DomainName|-dn> domain_name
[<-SecurityDomain |-sdn> security_domain]
[<-recipientSecurityDomain|-rdn> recipient_security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectNames|-pn> project_name_list
<-Permission|-pm> permission_name
<-RecipientName|-rn> recipient_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs ManageUserPermissionOnProject options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.  If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-recipientSecurityDomain -rdn	recipient_security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the recipient user belongs.  To set the recipient security domain, refer to the same guidelines that you use to set the security domain for the authorizing user.

Option	Argument	Description
-UserName -un	user_name	<p>Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.</p> <p>Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.</p>
-Password -pd	password	<p>Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.</p>
-ServiceName -sn	service_name	<p>Required. Model Repository Service name.</p>
-ProjectNames -pn	project_name_list	<p>Required. Names of the projects for which you want to allow or revoke permissions.</p> <p>The project names are not case sensitive.</p> <p>Separate multiple project names with a comma.</p>
-Permission -pm	permission_name	<p>Required. The permissions that you want to allow or revoke from the recipient group.</p> <p>Enter the permission in double quotes and use a backslash ( \ ) as the escape character.</p> <p>The following arguments are valid:</p> <p>+r, +w, +g, -r, -w, -g</p> <p>Use these arguments to allow or revoke read, write, and grant permissions.</p> <p>For example, a valid argument to revoke read permissions and allow write permissions is \ "-r+w\".</p>
-RecipientName -rn	recipient_name	<p>Required. The user name of the recipient user for which you want to manage permissions.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.</p>

# PopulateVCS

Synchronisiert das Modellrepository mit einem Versionsverwaltungssystem. Bevor Sie das Modellrepository mit einem Versionsverwaltungssystem synchronisieren, konfigurieren Sie Versionierungseigenschaften.

Wenn Sie Versionierungseigenschaften konfigurieren, starten Sie das Modellrepository neu und führen dann den Befehl „PopulateVCS“ aus.

**Hinweis:** Nach der Ausführung des Befehls ist das Modellrepository bis zum Abschluss der Synchronisierung nicht verfügbar.

Der Befehl „infacmd mrs populateVCS“ verwendet die folgende Syntax:

```
infacmd mrs populateVcs
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs populateVCS“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## ReassignCheckedOutObject

Weist die Eigentümerschaft eines ausgecheckten Objekts einem anderen Benutzer neu zu. Wenn der Eigentümer eines ausgecheckten Objekts die Änderungen gespeichert hat, werden diese beim erneuten Zuweisen des Objekts beibehalten. Werden die Änderungen nicht gespeichert, gehen sie beim erneuten Zuweisen des Objekts verloren.

Der Befehl „infacmd mrs reassignCheckedOutObject“ verwendet die folgende Syntax:

```
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ObjectPathandName|-opn> object_path_and_name
<-ToUser|-tu> to_user
[<-ToUserSecurityDomain|-tsd> to_user_security_domain]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs reassignCheckedOutObject“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ObjectPathAndName -opn	MRS_object_path	Erforderlich. Verwenden Sie folgende Syntax: ProjectName/FolderName/.../SubFolder_Name/ {ObjectName ProjectName/ObjectName}
-ToUser -tu	Benutzername	Erforderlich. Benutzername des Benutzers, der Besitzer des ausgecheckten Status des Objekts sein soll.
-ToUserSecurityDomain -tsd	Sicherheitsdomäne	Optional. Sicherheitsdomäne des Benutzers, der Besitzer des ausgecheckten Status des Objekts sein soll.

## rebuildDependencyGraph

Erstellt die Objektabhängigkeitsgrafik erneut, damit Sie die Objektabhängigkeiten nach einem Upgrade anzeigen können. Führen Sie diesen Befehl aus, wenn beim Upgrade des Modellrepository-Diensts die erneute Erstellung der Objektabhängigkeitsgrafik fehlgeschlagen ist.

Benutzer dürfen nicht auf Modellrepository-Objekte zugreifen, solange der Neuerstellungsvorgang nicht abgeschlossen ist, damit die Objektabhängigkeitsgrafik nicht ungenau wird. Diesen Befehl möchten Sie möglicherweise ausführen, wenn keine Benutzer angemeldet sind.

Der Befehl „infacmd mrs rebuildDependencyGraph“ verwendet die folgende Syntax:

```
rebuildDependencyGraph
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs rebuildDependencyGraph“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Dienst.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## RenameFolder

Benennt einen Ordner in einem Projekt um.

Der infacmd mrs RenameFolder-Befehl verwendet die folgende Syntax:

```
infacmd mrs renameFolder
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
<-SourceFolder|-sf> source_folder
<-TargetFolder|-tn> target_folder
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```



In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs RenameFolder“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
-ProjectName -pn	project_name	Erforderlich. Name des Projekts, das den umzubenennenden Ordner enthält.
-SourceFolder -sf	source_folder_path_and_name	Erforderlich. Pfad und Name des umzubenennenden Ordners. Pfad muss mit einem Schrägstrich (/) beginnen.

Option	Argument	Beschreibung
-TargetFolder -tn	target_folder_path_and_name	Erforderlich. Neuer Name für den Ordner. Sie können einen Ordernamen oder einen Pfad und Ordernamen angeben. Der Pfad muss mit einem Schrägstrich (/) beginnen.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## replaceMappingHadoopRuntimeConnections

Ersetzt die Hadoop-Verbindung aller Mappings im Repository durch eine andere Hadoop-Verbindung. Der Datenintegrationsdienst verwendet die Hadoop-Verbindung zum Verbinden mit dem Hadoop-Cluster, um Mappings in der Hadoop-Umgebung auszuführen.

Der Befehl ändert keine Hadoop-Verbindungen in den Umwandlungen. Sie können den Projektnamen angeben, um die Hadoop-Verbindung der Mappings im Projekt zu ersetzen.

Der Befehl infacmd mrs replaceMappingHadoopRuntimeConnections verwendet die folgende Syntax:

```
replaceMappingHadoopRuntimeConnections
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ProjectName|-pn> project_name]
<-OldConnectionName|-oc> connection_name_of_old_connection_to_replace
<-NewConnectionName|-nc> connection_name_of_new_connection
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente von `replaceMappingHadoopRuntimeConnections` beschrieben:

Option	Argument	Beschreibung
DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
Passwort -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts.
ProjectName -an	application_name	Optional. Name des Projekts, das das Mapping enthält. Wenn Sie diese Option angeben, ersetzt der Befehl die Hadoop-Verbindung nur für das Projekt.
OldConnectionName -oc	connection_name_of_old_connection_to_replace	Erforderlich. Name der Hadoop-Verbindung, die Sie ersetzen möchten.
NewConnectionName -nc	connection_name_of_new_connection	Erforderlich. Name der Hadoop-Verbindung, die vom Datenintegrationsdienst verwendet werden muss, um eine Verbindung mit dem Hadoop-Cluster für die Ausführung von Mappings in Hadoop herzustellen.
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

## RestoreContents

Stellt den Inhalt eines Modellrepository aus einer Backup-Datei wieder her.

Der Befehl „infacmd mrs RestoreContents“ verwendet die folgende Syntax:

```
RestoreContents
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
```

```

<-Password|-pd> password

<-ServiceName|-sn> service_name

<-InputFileName|-if> input_file_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs RestoreContents“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des zu sichernden Modellrepository-Diensts.
InputFileName -if	input_file_name	Erforderlich. Name der wiederherzustellenden Backup-Datei.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## UndoCheckout

Kehrt das Auschecken eines Modellrepository-Objekts um. Das Objekt wird in das Modellrepository eingchecked. Das Modellrepository verwirft alle Änderungen, die am Objekt vorgenommen wurden, seit es ausgecheckt wurde. Das Versionsverwaltungssystem erhöht die Versionsnummer nicht bzw. fügt sie nicht der Versionshistorie hinzu.

Der Befehl „infacmd mrs undoCheckout“ verwendet die folgende Syntax:

```
infacmd mrs undoCheckout
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ObjectPathAndName|-opn> Object_path_and_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs undoCheckout“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ObjectPathAndName -opn	MRS_object_path	Erforderlich. Pfad zum Modellrepository-Objekt, einschließlich Objektname. Setzen Sie den Pfad in doppelte Anführungszeichen. Verwenden Sie folgende Syntax: "ProjectName/FolderName/.../SubFolder_Name/{ObjectName ProjectName/ObjectName}"

## setMappingExecutionEnvironment

Gibt die Ausführungsumgebung für Zuordnungen an, die Sie über das Developer Tool ausführen.

Verwenden Sie Filter, um ein oder mehrere Mappings in einem Projekt zu aktualisieren. Wenn Sie keine Filter einschließen, aktualisiert der Befehl alle Mappings, die nicht im Datenintegrationsdienst bereitgestellt werden. Damit ein Mapping geändert werden kann, muss es allen festgelegten Filtern entsprechen.

Der Befehl infacmd mrs setMappingExecutionEnvironment verwendet die folgende Syntax:

```
setMappingExecutionEnvironment
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ProjectName|-pn> project_name]
[<-MappingNamesFilter|-mnf> mapping_names]
<-ExecutionEnvironment|-ee> execution_environment_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```



In der folgenden Tabelle werden die Optionen und Argumente von setMappingExecutionEnvironment beschrieben:

Option	Argument	Beschreibung
DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
Passwort -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
ProjectName -pn	project_name	Optional. Name des Projekts, das das Mapping enthält. Wenn Sie keinen Projektnamen angeben, aktualisiert der Befehl alle Projekte im Modellrepository.

Option	Argument	Beschreibung
MappingNamesFilter -mnf	mapping_names	Optional. Die Namen der Mappings, für die Sie die Ausführungsumgebung festlegen möchten. Trennen Sie die Namen der Mappings durch Kommas.  Standardwert sind alle nicht bereitgestellten Zuordnungen.
ExecutionEnvironment -ee	execution_environment_name	Erforderlich. Name der Ausführungsumgebung, die festgelegt werden soll. Wählen Sie entweder „Nativ“, „Hadoop“ oder „Databricks“ aus.
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

## UndoCheckout

Kehrt das Auschecken eines Modellrepository-Objekts um. Das Objekt wird in das Modellrepository eingchecked. Das Modellrepository verwirft alle Änderungen, die am Objekt vorgenommen wurden, seit es ausgecheckt wurde. Das Versionsverwaltungssystem erhöht die Versionsnummer nicht bzw. fügt sie nicht der Versionshistorie hinzu.

Der Befehl „infacmd mrs undoCheckout“ verwendet die folgende Syntax:

```
infacmd mrs undoCheckout
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ObjectPathAndName|-opn> Object_path_and_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs undoCheckout“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ObjectPathAndName -opn	MRS_object_path	Erforderlich. Pfad zum Modellrepository-Objekt, einschließlich Objektname. Setzen Sie den Pfad in doppelte Anführungszeichen. Verwenden Sie folgende Syntax: "ProjectName/FolderName/.../SubFolder_Name/{ObjectName ProjectName/ObjectName}"

## UnlockObject

Entsperrt ein Modellrepository-Objekt, das von einem Benutzer gesperrt wurde. Führen Sie diesen Befehl für ein Repository aus, das nicht in ein Versionsverwaltungssystem integriert ist.

**Hinweis:** Wenn Sie diesen Befehl für ein versioniertes Repository ausführen, schlägt der Befehl fehl.

Sie können jeweils ein Objekt entsperren.

Der Befehl „infacmd mrs unlockObject“ verwendet die folgende Syntax:

```
infacmd mrs unlockObject
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ObjectPathAndName|-opn> Object_path_and_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs unlockObject“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ObjectPathAndName -opn	MRS_object_path	Erforderlich. Pfad zum Modellrepository-Objekt, einschließlich Objektname. Verwenden Sie zum Beispiel die folgende Syntax: ProjectName/FolderName/SubFolder_Name/ ObjectName

## UpdateServiceOptions

Aktualisiert Optionen für den Modellrepository-Dienst. Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Der Befehl „infacmd mrs UpdateServiceOptions“ verwendet die folgende Syntax:

```
UpdateServiceOptions
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Options|-o> options
[<-PrimaryNode|-nn> primary node name]
[<-BackupNode|-bn> nodename1,nodename2,...]
[<-SearchIndexRoot|-si> search_index_root]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs UpdateServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Options -o	options	Erforderlich. Geben Sie Name-Wert-Paare durch Leerzeichen getrennt ein.
-PrimaryNode -nn	Name des primären Knotens	Optional. Knoten, auf dem der Modellrepository-Dienst ausgeführt werden soll.
-BackupNodes -bn	nodename1,nodename2,...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Backup-Knoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.
-SearchIndexRoot -si		Optional. Ändert das Verzeichnis für den Suchindex. Geben Sie den vollständigen Pfad zum Verzeichnis ein. Standardmäßig wird das Informatica-Installationsverzeichnis verwendet.

## Optionen des Modellrepository-Diensts

Verwenden Sie die Modellrepository-Dienst-Optionen mit dem Befehl „infacmd mrs UpdateServiceOptions“.

Geben Sie Modellrepository-Dienst-Optionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.



In der folgenden Tabelle werden die Modellrepository-Dienst-Optionen beschrieben:

Option	Argument	Beschreibung
CACHE.EnableCache	true   false	Aktiviert den Modellrepository-Dienst für die Speicherung von Modellrepository-Objekten im Cachespeicher. Starten Sie den Modellrepository-Dienst neu, um die Änderungen zu übernehmen.
CACHE.CacheJVMOptions	-Xmx[heap_size]	JVM-Optionen für den Modellrepository-Dienst-Cache. Konfigurieren Sie die maximale Heap-Größe, um die Speichermenge zu konfigurieren, die dem Cache zugewiesen wird. Dieses Feld muss die maximale Heap-Größe, angegeben durch die Option -Xmx, umfassen. Der Standard- und Mindestwert für die maximale Heap-Größe ist -Xmx128m.  Die von Ihnen konfigurierten Optionen werden beim Aktivieren des Modellrepository-Dienst-Cache übernommen. Starten Sie den Modellrepository-Dienst neu, um die Änderungen zu übernehmen. Die in diesem Feld konfigurierten Optionen gelten nicht für die JVM, die den Modellrepository-Dienst ausführt.
PERSISTENCE_DB.Username	db_user	Erforderlich. Konto für die Repository-Datenbank. Richten Sie dieses Konto mithilfe des Datenbank-Clients ein.
PERSISTENCE_DB.Password	db_password	Erforderlich. Passwort der Repository-Datenbank für den Datenbankbenutzer.
PERSISTENCE_DB.DatabaseSchema	db_schema	Optional. Der Name des Schemas für eine bestimmte Datenbank.
PERSISTENCE_DB.DatabaseTablespace	db_tablespace	Nur für eine DB2-Datenbank erforderlich. Beim Konfigurieren eines Tablespace-Namens erstellt der Modellrepository-Dienst alle Repository-Tabellen im selben Tablespace. Sie können im Tablespace-Namen keine Leerzeichen verwenden.  Bei einer IBM DB2-Datenbank mit mehreren Partitionen muss der Tablespace einen einzelnen Knoten und eine einzelne Partition umfassen.
PERSISTENCE_DB.DatabaseType	DatabaseType	Erforderlich. Zu den Datenbanktypen gehören: <ul style="list-style-type: none"> <li>- db2</li> <li>- oracle</li> <li>- mssqlserver</li> <li>- sybase</li> </ul>

Option	Argument	Beschreibung
PERSISTENCE_DB.JDBCConnectString	JDBC-Verbindungszeichenfolge	<p>Die JDBC-Verbindungszeichenfolge für die Verbindung mit der Modellrepository-Datenbank. Verwenden Sie die folgende Syntax für jede unterstützte Datenbank:</p> <ul style="list-style-type: none"> <li>- <b>IBM Db2.</b> "jdbc:informatica:db2://&lt;host name&gt;:&lt;port number&gt;;DatabaseName=&lt;database name&gt;;BatchPerformanceWorkaround=true;DynamicSections=3000"</li> <li>- <b>Microsoft SQL Server, der die Standardinstanz verwendet.</b> "jdbc:informatica:sqlserver://&lt;host name&gt;:&lt;port number&gt;;DatabaseName=&lt;database name&gt;;SnapshotSerializable=true"</li> <li>- <b>Microsoft SQL Server, der eine benannte Instanz verwendet.</b> "jdbc:informatica:sqlserver://&lt;host name&gt;\&lt;named instance name&gt;;DatabaseName=&lt;database name&gt;;SnapshotSerializable=true"</li> <li>- <b>Microsoft SQL Server, der die Standardinstanz mit Windows NT-Anmeldedaten verwendet.</b> "jdbc:informatica:sqlserver://&lt;host name&gt;:&lt;port number&gt;;DatabaseName=&lt;database name&gt;;SnapshotSerializable=true;authenticationMethod=NTLM"</li> <li>- <b>Microsoft SQL Server, der die benannte Instanz mit Windows NT-Anmeldedaten verwendet.</b> "jdbc:informatica:sqlserver://&lt;host name&gt;\&lt;named instance name&gt;;DatabaseName=&lt;database name&gt;;SnapshotSerializable=true;authenticationMethod=NTLM"</li> <li>- <b>Azure SQL Server.</b> "jdbc:informatica:sqlserver://&lt;host name&gt;:&lt;port number&gt;;DatabaseName=&lt;database name&gt;;SnapshotSerializable=true;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.&lt;hostname incertificate&gt;;ValidateServerCertificate=true"</li> <li>- <b>Azure SQL Database mit Active Directory-Authentifizierung.</b> "jdbc:informatica:sqlserver://&lt;host_name&gt;:&lt;port_number&gt;;database=&lt;database_name&gt;;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostnameInCertificate=*.database.windows.net;loginTimeout=&lt;seconds&gt;"</li> <li>- <b>Oracle.</b> "jdbc:informatica:oracle://&lt;host name&gt;:&lt;port number&gt;;SID=&lt;database name&gt;;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true"</li> </ul>

Option	Argument	Beschreibung
		<p>Zum Herstellen einer Verbindung zu Oracle mithilfe des Oracle-Verbindungsmanagers verwenden Sie folgende Verbindungszeichenfolge:</p> <pre>" jdbc:Informatica:oracle:TNSNamesFile=&lt;fully qualified path to the tnsnames.ora file&gt;;TNSServerName=&lt;TNS server name&gt;; "</pre> <p>- PostgreSQL.</p> <pre>"jdbc:informatica:postgresql://&lt;host name&gt;:&lt;port number&gt;;DatabaseName= "</pre>
PERSISTENCE_DB.SecureJDBCParameters	Sichere JDBC-Parameter	<p>Wenn die Modellrepository-Datenbank mittels SSL-Protokoll gesichert wird, müssen Sie die sicheren Datenbankparameter eingeben.</p> <p>Geben Sie die Parameter als name=value-Paare, getrennt durch ein Semikolon (;) ein. Beispiel:</p> <pre>param1=value1;param2=value2</pre>
PERSISTENCE_DB.Dialect	Dialekt	<p>Der SQL-Dialekt für eine bestimmte Datenbank. Der Dialekt ordnet Objekte zu Datenbankobjekten hinzu.</p> <p>Beispiel:</p> <pre>org.hibernate.dialect.Oracle9Dialect</pre>
PERSISTENCE_DB.Driver	Treiber	<p>Der Data Direct-Treiber zum Herstellen einer Verbindung zur Datenbank.</p> <p>Beispiel:</p> <pre>com.informatica.jdbc.oracle.OracleDriver</pre>
SEARCH.SearchAnalyzer	Vollständig qualifizierter Java-Klassenname	<p>Der vollständig qualifizierte Java-Klassenname des Search Analyzer.</p> <p>Standardmäßig verwendet der Modellrepository-Dienst den folgenden Search Analyzer für Englisch:</p> <pre>com.informatica.repository.service.provider.search.analysis.MMStandardAnalyzer</pre> <p>Der folgende Java-Klassenname kann für die Sprachen Chinesisch, Japanisch und Koreanisch angegeben werden:</p> <pre>org.apache.lucene.analysis.cjk.CJKAnalyzer</pre> <p>Alternativ können Sie einen benutzerdefinierten Search Analyzer erstellen.</p>
SEARCH.SearchAnalyzerFactory	Vollständig qualifizierter Java-Klassenname	<p>Vollständig qualifizierter Java-Klassenname der Factory-Klasse, wenn Sie eine Factory-Klasse zum Erstellen eines benutzerdefinierten Search Analyzer verwendet haben.</p> <p>Wenn Sie einen benutzerdefinierten Search Analyzer verwenden, geben Sie entweder den Namen der Search Analyzer-Klasse oder der Search Analyzer-Factory-Klasse ein.</p>

Option	Argument	Beschreibung
VCS.Host	„IP_address“ oder Hostname	<p>Erforderlich, um die Versionierungseigenschaften für das Modellrepository für Perforce zu konfigurieren.</p> <p>Die URL, die IP-Adresse oder der Hostname des Computers, auf dem das Perforce-Versionsverwaltungssystem ausgeführt wird.</p> <p>Verwenden Sie diese Option nicht mit SVN oder Git als Versionsverwaltungssystem.</p>
VCS.URL	URL des Subversion-Repositorys	<p>Erforderlich, um die Versioneigenschaften des Modellrepositorys auf SVN und Git zu konfigurieren.</p> <p>URL des Subversion-Repositorys. Beispiel:</p> <p>VCS.URL=https://myserver.company.com/svn/</p> <p>Verwenden Sie diese Option nicht, wenn Sie Perforce als Versionsverwaltungssystem konfigurieren.</p>
VCS.Port	VCS_port	<p>Erforderlich, um die Versionierungseigenschaften für das Modellrepository zu konfigurieren.</p> <p>Portnummer, die der Host des Versionsverwaltungssystems für das Abhören auf Pakete vom Modellrepository verwendet.</p>
VCS.User	VCS_user	<p>Erforderlich, um die Versionierungseigenschaften für das Modellrepository zu konfigurieren.</p> <p>Benutzerkonto für den Benutzer des Versionsverwaltungssystems.</p> <p>Dieses Konto muss über Schreibberechtigungen für das Versionsverwaltungssystem verfügen. Nachdem Sie die Verbindung mit diesem einzelnen Benutzer und Passwort für das Versionsverwaltungssystem konfiguriert haben, stellen alle Modellrepository-Benutzer die Verbindung zum Versionsverwaltungssystem über dieses Konto her.</p> <p>Für das Perforce-Versionsverwaltungssystem muss der Kontotyp ein Standardbenutzer sein.</p>
VCS.Password	VCS_password	<p>Erforderlich, um die Versionierungseigenschaften für das Modellrepository zu konfigurieren.</p> <p>Passwort für den Benutzer des Versionsverwaltungssystems.</p>

Option	Argument	Beschreibung
VCS.Type	VCS_type	<p>Erforderlich, um die Versionierungseigenschaften für das Modellrepository zu konfigurieren.</p> <p>Das unterstützte Versionsverwaltungssystem, mit dem Sie die Verbindung herstellen möchten. Sie können Perforce, SVN oder Git wählen.</p>
VCS.MRSPath	MRS_path	<p>Erforderlich, um die Versionierungseigenschaften für das Modellrepository mit Perforce zu konfigurieren.</p> <p>Pfad zum Root-Verzeichnis der Kopie von Modellrepository-Objekten des Versionsverwaltungssystems.</p> <p><b>Hinweis:</b> Wenn Sie den Befehl ausführen, stellt das Modellrepository eine Verbindung zum Versionsverwaltungssystem her und generiert das angegebene Verzeichnis, falls noch kein Verzeichnis vorhanden ist.</p> <p>Dieses Verzeichnis kann nur für einen Modellrepository-Dienst verwendet werden.</p> <p>Verwenden Sie für Perforce die folgende Syntax:</p> <pre>//directory/path</pre> <p><code>directory</code> ist das Root-Verzeichnis von Perforce und <code>path</code> ist der Rest des Pfades zum Root-Verzeichnis des Modellrepository-Objekts.</p> <p>Beispiel:</p> <pre>//depot/Informatica/repository_copy</pre> <p>Verwenden Sie diese Option nicht mit SVN oder Git als Versionsverwaltungssystem.</p>

## UpdateServiceProcessOptions

Aktualisiert Dienstprozessoptionen für den Modellrepository-Dienst. Trennen Sie mehrere Optionen mit einem Leerzeichen. Um einen Wert einzugeben, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Wert in Anführungszeichen.

Geben Sie Dienstprozessoptionen im folgenden Format ein:

```
... -o "option_name=value option_name=value" ...
```

Schließen Sie alle Optionsnamen und Werte in doppelte Anführungszeichen ein.

Der Befehl „`infacmd mrs UpdateServiceProcessOptions`“ verwendet die folgende Syntax:

```
UpdateServiceProcessOptions
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
```

```

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Options|-o> options

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs UpdateServiceProcessOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domännennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domännennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
NodeName -nn	Knotenname	Erforderlich. Der Knotenname, für den die Prozessoptionen festgelegt werden sollen.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomännennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariablen INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Options -o	options	Erforderlich. Geben Sie Name/Wert-Paare durch Leerzeichen getrennt ein. Geben Sie die Optionen in folgendem Format ein:  OptionGroupName.OptionName=OptionValue OptionGroupName2.OptionName2=OptionValue2

## UpdateStatistics

Aktualisiert die Statistiken für das Modellrepository auf Microsoft SQL Server. Sie können diesen Befehl ausführen, wenn Sie über die Systemadministratorberechtigung für die Microsoft SQL Server-Datenbank verfügen.

Der Befehl „infacmd mrs updateStatistics“ verwendet die folgende Syntax:

```
updateStatistics
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für `infacmd mrs updateStatistics` beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.



Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## UpgradeContents

Aktualisiert den Inhalt des Modellrepository. Der Befehl schlägt fehl, wenn das Modellrepository keinen Repository-Inhalt aufweist.

Der Befehl „infacmd mrs UpgradeContents“ verwendet die folgende Syntax:

```
UpgradeContents
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs UpgradeContents“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Dienst.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## UpgradeExportedObjects

Aktualisiert Objekte, die aus einer früheren Informatica-Version in eine XML-Datei im aktuellen Metadaten-Format exportiert wurden. Der Befehl generiert dann eine XML-Datei, die die aktualisierten Objekte enthält.

Der Befehl aktualisiert Objekte, die aus dem Modellrepository exportiert wurden. Importieren Sie die XML-Datei, die die aktualisierten Objekte enthält, in ein Modellrepository der aktuellen Version.

Der Aktualisierungsprozess hängt vom Modellrepository-Dienst ab. Sie müssen den Dienstnamen eines Modellrepository-Diensts angeben, der innerhalb der Domäne ausgeführt wird, wenn Sie den Befehl ausführen.

Der Befehl infacmd mrs UpgradeExportedObjects verwendet die folgende Syntax:

```
UpgradeExportedObjects
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-SourceFile|-sf> source_file
<-TargetFile|-tf> target_file
[<-OverwriteFile|-ow> overwrite_file]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für `infacmd mrs UpgradeExportedObjects` beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name eines Modellrepository-Diensts, der innerhalb der Domäne ausgeführt wird.
-SourceFile -sf	source_file	Erforderlich. Pfad und Dateiname der XML-Datei, die die zu aktualisierenden Objekte enthält. Sie können einen absoluten Pfad oder einen relativen Pfad zu der Datei angeben.

Option	Argument	Beschreibung
-TargetFile -tf	target_file	Erforderlich. Pfad und Dateiname der generierten XML-Datei, die die aktualisierten Objekte enthält. Sie können einen absoluten Pfad oder einen relativen Pfad zu der Datei angeben.
OverwriteFile -ow	overwrite_file	Optional. Sie müssen diese Option einbeziehen, um die Zielfeile mit demselben Namen zu überschreiben.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## KAPITEL 26

# infacmd ms-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [abortAllJobs, 970](#)
- [deleteMappingPersistedOutputs, 972](#)
- [fetchAggregatedClusterLogs, 975](#)
- [getMappingStatus, 977](#)
- [getRequestLog, 979](#)
- [ListMappingOptions, 981](#)
- [listMappingParams, 982](#)
- [listMappingPersistedOutputs, 985](#)
- [listMappings, 987](#)
- [purgeDatabaseWorkTables, 989](#)
- [runMapping, 991](#)
- [UpdateMappingOptions, 996](#)
- [UpdateOptimizationDefaultLevel, 998](#)
- [UpdateOptimizationLevel, 1000](#)
- [UpgradeMappingParameterFile, 1002](#)

## abortAllJobs

Bricht alle Zuordnungsjobs ab, die für den Datenintegrationsdienst bereitgestellt werden.

Der Befehl wirkt sich auf bereitgestellte Jobs aus, die für die Ausführung auf der Spark-Engine konfiguriert sind. Der Befehl wirkt sich auf Jobs in der Warteschlange aus, die in dem Modellrepository gespeichert sind, das in den Eigenschaften des Datenintegrationsdiensts konfiguriert ist. Der Befehl bricht Batch-Jobs ab, die Sie mit infacmd ausführen.

Für On-Demand-Jobs bricht der Befehl Jobs auf einem der Datenintegrationsdienst-Knoten ab, was keine Auswirkungen auf andere Domänenknoten hat.

**Hinweis:** Es ist nicht möglich, den Knoten anzugeben, auf dem der Befehl On-Demand-Jobs abbricht.

Sie können optionale Flags verwenden, um den Befehl nur auf Jobs in der Warteschlange oder auf ausgeführte Jobs anzuwenden. Wenn Sie keine der Optionen verwenden, wirkt sich der Befehl auf alle Jobs aus.

Der Befehl schlägt fehl, wenn er während der Spark-Bereinigung ausgeführt wird.

Der Befehl „infacmd ms abortAllJobs“ verwendet folgende Syntax:

```
abortAllJobs
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-OnlyQueuedJobs|-q> true|false]
[<-OnlyRunningJobs|-r> true|false]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms abortAllJobs“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-OnlyQueuedJobs -q	true   false	Optional. Verwenden Sie diese Option, um die betreffenden Jobs so zu filtern, dass nur die vom Datenintegrationsdienst zur Ausführung in die Warteschlange gestellten Jobs aufgenommen werden.
-OnlyRunningJobs -r	true   false	Optional. Verwenden Sie diese Option, um die betreffenden Jobs so zu filtern, dass nur die vom Datenintegrationsdienst ausgeführten Jobs aufgenommen werden.

## deleteMappingPersistedOutputs

Löscht alle persistenten Zuordnungsausgaben für eine bereitgestellte Zuordnung. Geben Sie die zu löschenden Ausgaben anhand des Namens der Anwendung und des Namens der Laufzeitinstanz der Zuordnung an. Um bestimmte Ausgaben zu löschen, verwenden Sie die Option -OutputNamesToDelete.

Der Befehl „infacmd ms deleteMappingPersistedOutputs“ verwendet die folgende Syntax:

```
deleteMappingPersistedOutputs
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
```



```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-Application|-a> application_name

<-RuntimeInstanceName|-rin> runtime_instance_name

[<-OutputNamesToDelete|-ontd> output_names_to_delete]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms deleteMappingPersistedOutputs“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariablen INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Zuordnung ausgeführt hat.
-Application -a	application_name	Erforderlich. Name der Anwendung, die die Zuordnung enthält.
-RuntimeInstanceName -rin	runtime_instance_name	<p>Erforderlich. Name der Laufzeitinstanz der Zuordnung. Verwenden Sie den im Befehl „infacmd ms runMapping“ angegebenen Namen, um die Befehle „listMappingPersistedOutputs“ und „deleteMappingPersistedOutputs“ auszuführen.</p>
-OutputNamesToDelete -ontd	Zu löschende Ausgabenamen	Optional. Namen der dauerhaft zu löschenden Ausgaben. Um mehrere Ausgaben zum Löschen anzugeben, trennen Sie die Namen durch ein Komma.

# fetchAggregatedClusterLogs

Ruft die .zip- oder tar.gz-Datei der aggregierten Clusterprotokolle für eine Zuordnung basierend auf der Job-ID ab und schreibt die komprimierte aggregierte Protokolldatei in ein Zielverzeichnis.

Der Befehl „infacmd ms fetchAggregatedClusterLogs“ verwendet die folgende Syntax:

```
fetchAggregatedClusterLogs

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-RequestId|-id> request_id

[<-TargetLogDirectory|-tld> target_log_directory]

[<-TargetFilename|-tf> target_filename_without_extension]

[<-ClusterLoginUsername|-clu> cluster_login_username]

[<-ClusterLoginPassword|-clp> cluster_login_password]

[<-CustomProperties|-cp> custom_properties]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms fetchAggregatedClusterLogs“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Zuordnung ausgeführt hat.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariablen INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-RequestId -id	request_id	Erforderlich. Die Job-ID für die Zuordnung, für die die Protokolldatei geschrieben werden soll. Geben Sie die Job-ID ein, die der Befehl „infacmd ms runMapping“ zurückgibt.
-TargetLogDirectory -tld	Zielprotokollverzeichnis	Optional. Das Verzeichnis, in dem Sie die komprimierte aggregierte Protokolldatei speichern möchten.
-TargetFilename -tf	Zieldateiname ohne Erweiterung	Optional. Name und Dateipfad der komprimierten aggregierten Protokolldatei.
-ClusterLoginUsername -clu	Benutzername für die Clusteranmeldung	Erforderlich, wenn Sie die Kerberos-fähige Yarn-Ressourcenmanager-Anwendung verwenden. Benutzername für den Zugriff auf die YARN-Anwendung.

Option	Argument	Beschreibung
-ClusterLoginPassword -clp	Passwort für die Clusteranmeldung	Erforderlich, wenn Sie den Benutzernamen für die Cluster-Anmeldung angeben. Passwort für den Zugriff auf die YARN-Anwendung. Beim Passwort wird die Groß-/Kleinschreibung beachtet.
-CustomProperties -cp	custom_properties	Optional. Definieren Sie benutzerdefinierte Eigenschaften für eine Zuordnung auf Anfrage des globalen Kundensupports von Informatica. Geben Sie benutzerdefinierte Eigenschaften als durch Semikola getrennte Name/Wert-Paare ein. Beispiel:  ... -cp custom_property_name=value  Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

## getMappingStatus

Ruft den aktuellen Status eines bereitgestellten Mapping-Jobs nach Auftrags-ID ab. Geben Sie die Job-ID ein, die vom Befehl „infacmd ms runMapping“ zurückgegeben wurde.

**Hinweis:** Sie müssen den überwachenden Modellrepository-Dienst im Administrator Tool konfigurieren, bevor Sie diesen Befehl verwenden.

Der Befehl „infacmd ms getMappingStatus“ verwendet folgende Syntax:

```
getMappingStatus
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-ServiceName|-sn> service_name
<-JobId|-ji> job_id
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

Der Befehl gibt Informationen über eine Zuordnungsausführung, einschließlich Jobname, Jobsatus und Protokolldateipfad, zurück.

Wenn mit dem Befehl runMapping ein Name der Laufzeitinstanz übergeben wurde, ist der Jobname der Name der Laufzeitinstanz. Anderenfalls ist der Jobname eine der folgenden Optionen:

- <mapping name>
- <mapping name>\_<parameter set name>
- <mapping name>\_<parameter file name>

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms getMappingStatus“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Zuordnung ausgeführt hat.

Option	Argument	Beschreibung
-JobId -jI	job_id	Erforderlich. Die Job-ID für das Mapping, dessen Status Sie abrufen möchten. Geben Sie die Job-ID ein, die vom Befehl „infacmd ms runMapping“ zurückgegeben wurde.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariablen INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## getRequestLog

Schreibt das Zuordnungsprotokoll in die angegebene Datei. Geben Sie die Job-ID ein, die vom Befehl „infacmd ms runMapping“ zurückgegeben wurde.

Der Befehl „infacmd ms getRequestLog“ verwendet folgende Syntax:

```
getRequestLog
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-RequestId|-id> request_id
<-FileName|-f> file_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms getRequestLog“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Zuordnung ausgeführt hat.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-RequestId -id	request_id	<p>Erforderlich. Die Job-ID für die Zuordnung, für die die Protokolldatei geschrieben werden soll. Geben Sie die Job-ID ein, die vom Befehl „infacmd ms runMapping“ zurückgegeben wurde.</p>
-FileName -f	file_name	<p>Erforderlich. Name und Dateipfad, in den die Protokolldatei geschrieben werden soll.</p>



# ListMappingOptions

Listet Zuordnungsoptionen in einer Anwendung auf.

Der Befehl „`infacmd ms listMappingOptions`“ verwendet folgende Syntax:

```
listMappingOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-Mapping|-m> mapping_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd ms listMappingOptions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit diesen beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts zum Ausführen der Zuordnung. Die Anwendung, die die Zuordnung enthält, muss für einen Datenintegrationsdienst bereitgestellt werden.
-Application -a	application_name	Erforderlich. Name der Anwendung, die die Zuordnung enthält.
-Mapping -m	mapping_name	Erforderlich. Name der Zuordnung.

## listMappingParams

Listet die Parameter für ein Mapping auf und erstellt eine Mapping-Parameterdatei, die Sie beim Ausführen eines Mappings verwenden können. Der Befehl gibt eine XML-Datei mit Standardwerten zurück, die Sie aktualisieren können. Geben Sie den Namen der Parameterdatei ein, wenn Sie die Zuordnung mit „infacmd ms runMapping“ ausführen.

Der Befehl „infacmd ms listMappingParams“ verwendet folgende Syntax:

```
listMappingParams
<-DomainName|-dn> domain_name
```

```

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application_name

<-Mapping|-m> mapping_name

[<-OutputFile|-o> output_file_to_write_to]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms listMappingParams“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts zum Ausführen der Zuordnung. Die Anwendung, die die Zuordnung enthält, muss für einen Datenintegrationsdienst bereitgestellt werden.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung, die die Zuordnung enthält.
-Mapping -m	mapping_name	Erforderlich. Name der Zuordnung.
- OutputFile - o	output file_to_write_to	Optional. Pfad und Dateiname der zu erstellenden Parameterdatei. Wenn Sie keine Datei angeben, zeigt der Befehl die Parameter in der Eingabeaufforderung an.

## listMappingParams-Ausgabe

Der Befehl „listMappingParams“ gibt eine Parameterdatei als XML-Datei mit Standardwerten zurück, die Sie aktualisieren können.

Sie führen beispielsweise den Befehl „listMappingParams“ für die Anwendung „MyApp“ und die Zuordnung „MyMapping“ aus. Das Mapping "MyMapping" hat einen Parameter "MyParameter". Der Befehl „listMappingParams“ gibt eine XML-Datei in folgendem Format zurück:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<root xmlns="http://www.informatica.com/Parameterization/1.0" xmlns:xsi="http://
www.w3.org/2001/XMLSchema">
  <!--
    <application name="MyApp">
      <mapping name="MyMapping">
        <!-- Specify deployed application specific parameters here. -->
      </mapping>
    </application>
  -->
```

```

    <project name="MyProject">
      <mapping name="MyMapping">
        <parameter name="MyParameter">DefaultValue</parameter>
      </mapping>
    </project>
  </root>

```

Die Ausgabe-XML-Datei hat die folgenden Elemente der obersten Ebene:

#### Anwendungselement

Wenn Sie einen Parameter innerhalb des Elements auf der obersten Ebene einer Anwendung definieren, wendet der Data Integration Service den Parameterwert an, wenn Sie das angegebene Mapping in der angegebenen Anwendung ausführen. Sie müssen mindestens ein Projektelement in eine Anwendung/ein Mapping-Element einbeziehen.

Standardmäßig befindet sich dieses Element auf der obersten Ebene in den Kommentaren. Entfernen Sie die Kommentare (!-- and -->), um dieses Element zu verwenden.

#### Projektelement

Wenn Sie einen Parameter innerhalb des Elements auf der obersten Ebene eines Projekts definieren, wendet der Data Integration Service den Parameterwert auf das angegebene Mapping im Projekt in jeder bereitgestellten Anwendung an. Der Dienst wendet den Parameterwert auch auf alle Mappings an, die die Objekte im Projekt verwenden.

Wenn Sie in einem Projekt denselben Parameter in einem Element auf der obersten Ebene einer Anwendung und ein Element in derselben Parameterdatei definieren, hat der im Anwendungselement definierte Parameterwert Vorrang.

## listMappingPersistedOutputs

Listet die persistenten Zuordnungsausgaben für eine bereitgestellte Zuordnung auf. Die Ausgaben werden basierend auf dem Namen der Anwendung und dem Namen der Laufzeitinstanz der Zuordnung aufgelistet.

Der Befehl „`infacmd ms listMappingPersistedOutputs`“ verwendet die folgende Syntax:

```

listMappingPersistedOutputs
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Application|-a> application_name
<-RuntimeInstanceName|-rin> runtime_instance_name

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms listMappingPersistedOutputs“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariablen INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Zuordnung ausgeführt hat.
-Application -a	application_name	Erforderlich. Name der Anwendung, die die Zuordnung enthält.
-RuntimeInstanceName -rin	runtime_instance_name	Erforderlich. Name der Laufzeitinstanz der Zuordnung. Verwenden Sie den im Befehl „infacmd ms runMapping“ angegebenen Namen, um die Befehle „listMappingPersistedOutputs“ und „deleteMappingPersistedOutputs“ auszuführen.

## listMappings

Listet die Mappings in einer Anwendung auf.

Der Befehl „infacmd ms listMappings“ verwendet folgende Syntax:

```
listMappings
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Application|-a> application_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms listMappings“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit diesen beiden Methoden festlegen, hat die Option -re Vorrang.



Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts zum Ausführen der Zuordnung. Die Anwendung, die die Zuordnung enthält, muss für einen Datenintegrationsdienst bereitgestellt werden.
-Application -a	application_name	Erforderlich. Name der Anwendung, die die Zuordnung enthält.

## purgeDatabaseWorkTables

Löscht alle Jobinformationen aus der Warteschlange, wenn Sie die Data-Engineering-Wiederherstellung für den Datenintegrationsdienst aktivieren.

Der Befehl löscht Arbeitswarteschlangen, bestimmte Informationen zu ausgeführten Jobs sowie Informationen zur Data-Engineering-Wiederherstellung. Der Befehl entfernt Zeilen aus Datenbanktabellen von in der Warteschlange befindlichen und ausgeführten Jobs. Verwenden Sie den Befehl zum Entfernen restlicher Jobinformationen in der Datenbank des Modellrepositorys, nachdem Sie den für die Data-Engineering-Wiederherstellung konfigurierten Datenintegrationsdienst gelöscht haben.

Der Befehl wirkt sich auf Jobs in dem Modellrepository aus, das in den Eigenschaften des Datenintegrationsdiensts konfiguriert ist. Sie können die Option -msn zum Angeben eines anderen Modellrepositorys verwenden.

Sie können die Option -q verwenden, um den Befehl ausschließlich auf in der Warteschlange befindliche Jobs anzuwenden.

Sie können den Befehl nur ausgeben, wenn der Datenintegrationsdienst angehalten wird.

Der Befehl „infacmd ms purgeDatabaseWorkTables“ verwendet folgende Syntax:

```

purgeDatabaseWorkTables
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-OnlyQueuedJobs|-q> true|false]
[<-MrsName|-msn> mrs_service_name]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms purgeDatabaseWorkTables“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariablen INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

Option	Argument	Beschreibung
-OnlyQueuedJobs -q	true   false	Optional. Verwenden Sie diese Option, um die Ergebnisse so zu filtern, dass nur die vom Datenintegrationsdienst zur Ausführung in die Warteschlange gestellten Jobs aufgenommen werden.
-MrsName -msn	Model_repository_service_name	Optional. Name des Modellrepository-Diensts, aus dem Datenbankarbeitstabellen gelöscht werden sollen.  Verwenden Sie diese Option nur zum Löschen von Datenbankarbeitstabellen, wenn der Datenintegrationsdienst gelöscht wird. Mit dieser Option werden alle Zeilen dauerhaft aus den Arbeitstabellen gelöscht.

## runMapping

Führt eine Zuordnung aus, die einem Datenintegrationsdienst bereitgestellt wird. Sie können die Zuordnung mit einem Parametersatz oder einer Parameterdatei ausführen.

Führen Sie zum Erstellen einer Parameterdatei für eine Zuordnung den Befehl „`infacmd ms listMappingParams`“ aus. Führen Sie zuerst den Befehl „`infacmd dis startApplication`“ für die Anwendung und dann den Befehl „`infacmd ms listMappingParams`“ aus.

Führen Sie zum Anzeigen der Parameter und Werte für einen Parametersatz den Befehl „`infacmd dis listParameterSetEntries`“ aus.

Der Befehl „`infacmd ms runMapping`“ verwendet folgende Syntax:

```
runMapping
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-Mapping|-m> mapping_name
[<-Wait|-w> true|false]
[<-ParameterFile|-pf> parameter_file_path]
[<-ParameterSet|-ps> parameter_set_name]
[<-OperatingSystemProfile|-osp> operating_system_profile_name]
[<-NodeName|-nn> node_name]
[<-OptimizationLevel|-ol> optimization_level]
```

```
[<-PushdownType|-pt> pushdown_type]

[<-RuntimeInstanceName|-rin> runtime_instance_name]

[<-EnableAudit|-ea> true|false]

[<-CustomProperties|-cp> custom_properties]
```

Der Befehl gibt die Job-ID für die Zuordnungsausführung zurück.

Sie müssen die Überwachung aktivieren, um den Namen der Laufzeitinstanz zu speichern. Wenn Sie die Überwachungsstatistiken bereinigen, werden die Namen der Laufzeitinstanz gelöscht und nicht vom Befehl „infacmd ms getMappingStatus“ zurückgegeben. Das Zuordnungsprotokoll kann weiterhin den Namen der Laufzeitinstanz enthalten und die dem Namen der Laufzeitinstanz zugeordneten beibehaltenen Zuordnungsausgaben können weiterhin verwendet werden.

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms runMapping“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts zum Ausführen der Zuordnung. Die Anwendung, die die Zuordnung enthält, muss für einen Datenintegrationsdienst bereitgestellt werden.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-Application -a	application_name	Erforderlich. Name der Anwendung, die die Zuordnung enthält.
-Mapping -m	mapping_name	Erforderlich. Name der auszuführenden Zuordnung.
-Wait -w	true false	<p>Optional. Gibt an, ob infacmd bis zum Abschluss der Zuordnung wartet, bevor eine Rückkehr zur Shell oder Eingabeaufforderung erfolgt. Ist die Option auf TRUE festgelegt, kehrt infacmd nach Abschluss der Zuordnung zur Shell oder Eingabeaufforderung zurück. Sie können keine nachfolgenden Befehle ausführen, wenn die Zuordnung noch nicht abgeschlossen ist. Ist die Option auf FALSE festgelegt, kehrt infacmd sofort zur Shell oder Eingabeaufforderung zurück. Sie müssen nicht auf den Abschluss der Zuordnung warten, bevor Sie den nächsten Befehl ausführen. Standardwert ist „false“.</p>
-ParameterFile -pf	parameter_file_path	Optional. Name und Pfad der Parameterdatei. Geben Sie weder eine Parameterdatei noch einen Parametersatz ein.
-ParameterSet -ps	parameter_set_name	Optional. Name eines zur Laufzeit zu verwendenden Parametersatzes. Die Parametersatzoption überschreibt alle mit einer Anwendung bereitgestellten Parametersätze. Geben Sie weder einen Parametersatz noch eine Parameterdatei ein.

Option	Argument	Beschreibung
-OperatingSystemProfile -osp	operating_system_profile_name	Optional. Name des Betriebssystemprofils, das die Zuordnung ausführt.  Wenn Sie diese Option nicht verwenden, wenn der Datenintegrationsdienst zur Verwendung von Betriebssystemprofilen eingerichtet ist, führt der Datenintegrationsdienst die Zuordnung mit dem Standardprofil aus.
-NodeName -nn	node_name	Optional. Name des Knotens in einem Datenintegrationsdienstgitter, an den der Zuordnungsjob gesendet werden soll. Ein Datenintegrationsdienstprozess muss auf dem Knoten ausgeführt werden.  Wenn Sie diese Option nicht verwenden, wird der Zuordnungsjob an den Knoten gesendet, auf dem der Master-Prozess des Datenintegrationsdiensts ausgeführt wird.
-OptimizationLevel -ol	optimization_level	Optional. Steuert die Optimierungsmethoden, die der Datenintegrationsdienst auf die Zuordnung anwendet. Geben Sie den numerischen Wert ein, der mit der Optimierungsebene verbunden ist, die Sie konfigurieren möchten. Geben Sie einen der folgenden Werte ein: <b>-1 (Auto)</b>  Der Datenintegrationsdienst wendet Optimierungen auf Basis des Ausführungsmodus und der Zuordnungsinhalte an. <b>0 (Keine)</b>  Der Datenintegrationsdienst wendet keine Optimierung an. <b>1 (Minimal)</b>  Der Datenintegrationsdienst wendet die Optimierungsmethode der frühen Projektion an. <b>2 (Normal)</b>  Der Datenintegrationsdienst wendet folgende Optimierungsmethoden an: frühe Projektion, frühe Auswahl, Verzweigungsbereinigung, Push-Into, globale Vorhersage und Vorhersage. <b>3 (Vollständig)</b>  Der Datenintegrationsdienst wendet folgende Optimierungsmethoden an: kostenbasiert, frühe Projektion, frühe Auswahl, Verzweigungsbereinigung, Vorhersage, Push-Into, Semi-Join und Dataship-Join.  Standardwert ist „-1 (Auto)“.

Option	Argument	Beschreibung
-PushdownType -pt	pushdown_type	<p>Optional. Steuert den Pushdown-Typ, den der Datenintegrationsdienst auf eine Zuordnung anwendet. Geben Sie einen der folgenden Werte ein:</p> <ul style="list-style-type: none"> <li>- Keine. Wählt keinen Pushdown-Typ für die Zuordnung aus.</li> <li>- Quelle. Der Datenintegrationsdienst versucht, möglichst viel Umwandlungslogik in die Quelldatenbank zu übertragen.</li> <li>- Vollständig. Der Datenintegrationsdienst überträgt die vollständige Umwandlungslogik in die Quelldatenbank.</li> </ul> <p>Diese Option überschreibt den Pushdown-Typ, der in den Laufzeiteigenschaften der Zuordnung oder in einer Parameterdatei oder einem -satz festgelegt wurde.</p> <p>Wenn Sie diese Option nicht verwenden, wendet der Datenintegrationsdienst den Pushdown-Typ an, der in den Laufzeiteigenschaften der Zuordnung oder in einer Parameterdatei oder einem -satz festgelegt wurde.</p>
-RuntimeInstanceName -rin	runtime_instance_name	<p>Optional. Name der Laufzeitinstanz der Zuordnung. Der Name muss eindeutig sein.</p> <p>Der Name der Laufzeitinstanz darf keine Schrägstriche ( / ) enthalten.</p> <p>Sie müssen in runMapping einen Namen für die Laufzeitinstanz angeben, um Zuordnungsausgaben beizubehalten und die Befehle listMappingPersistedOutputs und deleteMappingPersistedOutputs auszuführen.</p> <p><b>Tipp:</b> Sie können den Wert wie folgt festlegen, um die Namen der Laufzeitinstanz zu standardisieren:</p> <ul style="list-style-type: none"> <li>- Wenn alle Zuordnungen in einer Anwendung die selben beibehaltenen Zuordnungsausgaben verwenden, verwenden Sie den Anwendungsnamen.</li> <li>- Wenn die Zuordnungen verschiedene beibehaltene Zuordnungsausgaben verwenden, verwenden Sie eine Kombination aus Anwendungsname, Zuordnungsname und festgelegten Parameter oder Dateiname.</li> </ul>

Option	Argument	Beschreibung
-EnableAudit -ea	true false	Optional. Gibt an, ob die Auditregeln und -bedingungen mit der Zuordnung ausgeführt werden. Der Standardwert ist „false“. Diese Option überschreibt die Konfiguration <b>Audit aktivieren</b> im Developer Tool. Beispiel: Wenn Sie <b>Audit aktivieren</b> im Developer Tool auswählen und den Standardwert für diese Option verwenden, werden die Auditregeln und -bedingungen nicht ausgeführt.
-CustomProperties -cp	custom_properties	Optional. Definieren Sie benutzerdefinierte Eigenschaften für eine Zuordnung auf Anfrage des globalen Kundensupports von Informatica. Geben Sie benutzerdefinierte Eigenschaften als durch Semikola getrennte Namen-Wert-Paare ein. Beispiel: ... -cp custom_property_name=value Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

## UpdateMappingOptions

Aktualisiert Zuordnungsoptionen in einer Anwendung.

Der Befehl „infacmd ms updateMappingOptions“ verwendet folgende Syntax:

```
updateMappingOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Application|-a> application_name
<-Mapping|-m> mapping_name
<-Options|-o> options
```



In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms updateMappingOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit diesen beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts zum Ausführen der Zuordnung. Die Anwendung, die die Zuordnung enthält, muss für einen Datenintegrationsdienst bereitgestellt werden.
-Application -a	application_name	Erforderlich. Name der Anwendung, die die Zuordnung enthält.
-Mapping -m	mapping_name	Erforderlich. Name der Zuordnung.
-Options -o	options	Optional. Liste der zu konfigurierenden Optionen. Trennen Sie die einzelnen Optionen mit einem Leerzeichen. Führen Sie zum Anzeigen der Optionen den Befehl „infacmd as ListServiceOptions“ aus.

## UpdateOptimizationDefaultLevel

Aktualisiert die Optimierungsebene für alle Zuordnungen in einer Anwendung mit Optimierungsebene 2 (Normal) auf -1 (Auto). Vor Version 10.4.0 war „Normal“ die standardmäßige Optimierungsebene. Für alle neuen Zuordnungen ist „Auto“ der Standardwert. Der Befehl wirkt sich nicht auf Zuordnungen in der Anwendung aus, die eine andere Optimierungsebene als „Normal“ haben.

Der Befehl „infacmd ms updateOptimizationDefaultLevel“ verwendet die folgende Syntax:

```

updateOptimizationDefaultLevel

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application_name

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms updateOptimizationDefaultLevel“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts zum Ausführen der Zuordnung. Die Anwendung, die die Zuordnung enthält, muss für einen Datenintegrationsdienst bereitgestellt werden.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout bei beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung, die die Zuordnung(en) enthält.

## UpdateOptimizationLevel

Aktualisiert die Optimierungsebene für mehrere Zuordnungen in einer Anwendung.

Der Befehl „infacmd ms updateOptimizationLevel“ verwendet folgende Syntax:

```
updateoptimizationLevel
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
[<-Mapping|-m> mapping_name]
[<-OptimizationLevel|-ol> optimization_level]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms updateOptimizationLevel“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts zum Ausführen der Zuordnung. Die Anwendung, die die Zuordnung enthält, muss für einen Datenintegrationsdienst bereitgestellt werden.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout bei beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-Application -a	application_name	<p>Erforderlich. Name der Anwendung, die die Zuordnung(en) enthält.</p>

Option	Argument	Beschreibung
-Mapping -m	mapping_name	Optional. Name der zu ändernden Zuordnung. Zum Aktualisieren der Optimierungsebene für mehrere Zuordnungen trennen Sie jeden Zuordnungsamen durch ein Komma. Standardwert sind alle Zuordnungen in einer Anwendung.
-OptimizationLevel -ol	optimization_level	Optional. Die Optimierungsmethode, die vom Datenintegrationsdienst auf eine Zuordnung angewendet wird. Geben Sie einen der folgenden Werte ein: <b>-1 (Auto)</b> Der Datenintegrationsdienst wendet Optimierungen auf Basis des Ausführungsmodus und der Zuordnungsinhalte an. <b>0 (Keine)</b> Der Datenintegrationsdienst wendet keine Optimierung an. <b>1 (Minimal)</b> Der Datenintegrationsdienst wendet die Optimierungsmethode der frühen Projektion an. <b>2 (Normal)</b> Der Datenintegrationsdienst wendet folgende Optimierungsmethoden an: frühe Projektion, frühe Auswahl, Verzweigungsreinigung, Push-Into, globale Vorhersage und Vorhersage. <b>3 (Vollständig)</b> Der Datenintegrationsdienst wendet folgende Optimierungsmethoden an: kostenbasiert, frühe Projektion, frühe Auswahl, Verzweigungsreinigung, Vorhersage, Push-Into, Semi-Join und Dataship-Join. Standardwert ist „-1 (Auto)“.

## UpgradeMappingParameterFile

Wandelt eine in einer vorherigen Informatica-Version erstellte Parameterdatei in ein Parameterdateiformat um, das für Informatica Version 10.0 gültig ist.

In Informatica Version 10.0 kann eine Parameterdatei Zuordnungs- und Arbeitsablaufparameter, aber keine Umwandlungsparameter mehr enthalten. Wenn Sie eine Zuordnung oder einen Arbeitsablauf in der mit einer früheren Version erstellten Parameterdatei ausführen, muss der Datenintegrationsdienst die Parameterdatei zur Laufzeit in die Informatica Version 10.0 konvertieren. Sie können die Leistung steigern, indem Sie Parameterdateien in das Informatica 10.0-Format konvertieren.

Der `infacmd ms upgradeMappingParameterFile`-Befehl verwendet die folgende Syntax:

```
upgradeMappingParameterFile
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-Mapping|-m> mapping_name
[<-OutputFile|-o> output_file_to_write_to]
<-ParameterFile|-pf> parameter_file_to_upgrade
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd ms upgradeMappingParameterFile`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts zum Ausführen der Zuordnung. Die Anwendung, die die Zuordnung enthält, muss für einen Datenintegrationsdienst bereitgestellt werden.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung, die die Zuordnung enthält.
-Mapping -m	mapping_name	Erforderlich. Name der Zuordnung.
- OutputFile - o	output file_to_write_to	Optional. Pfad und Dateiname der zu erstellenden Parameterdatei. Wenn Sie keine Datei angeben, zeigt der Befehl die Parameter in der Eingabeaufforderung an.
-ParameterFile -pf	parameter_file_to_upgrade	Erforderlich. Der Name der zu aktualisierenden Parameterdatei.



## KAPITEL 27

# Infacmd oie-Befehlsreferenz

Das oie-Plug-In ist veraltet und Unterstützung für das oie-Plug-In wird in einer künftigen Version eingestellt. Die infacmd oie-Befehle wurden auf das Tools-Plug-In migriert. Die Befehlsbeschreibungen können unter [Kapitel 37, "infacmd tools-Befehlsreferenz" auf Seite 1224](#) angezeigt werden.

## KAPITEL 28

# infacmd ps-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [cancelProfileExecution, 1006](#)
- [CreateWH, 1008](#)
- [detectOrphanResults, 1010](#)
- [DropWH, 1011](#)
- [Execute, 1013](#)
- [executeProfile, 1015](#)
- [getExecutionStatus, 1017](#)
- [getProfileExecutionStatus, 1019](#)
- [List, 1021](#)
- [ListAllProfiles, 1023](#)
- [migrateProfileResults, 1024](#)
- [migrateScorecards, 1026](#)
- [Purge, 1028](#)
- [purgeOrphanResults, 1030](#)
- [restoreProfilesAndScorecards, 1032](#)
- [synchronizeProfile, 1034](#)

## cancelProfileExecution

Stoppt alle Profilausführungen, einschließlich der Profile sowie des Enterprise-Erkennungsprofils.

Der Befehl „infacmd ps cancelProfileExecution“ verwendet die folgende Syntax:

```
cancelProfileExecution  
  
<-DomainName|-dn> domain_name  
  
[<-Gateway|-hp> gateway_name]  
  
[<-NodeName|-nn> node_name]  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]

<-MrsServiceName|-msn> MRS_name

<-DsServiceName|-dsn> data_integration_service_name

<-ObjectPathAndName|-opn> MRS_object_path
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd ps cancelProfileExecution“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-DsServiceName -dsn	data_integration_service_name	Erforderlich. Name des Datenintegrationsdiensts.
-ObjectPathAndName -opn	MRS_object_path	<p>Erforderlich. Verwenden Sie folgende Syntax:</p> <pre>ProjectName/FolderName/.../SubFolder_Name/ {ObjectName ProjectName/ObjectName}</pre>

## CreateWH

Erstellt den Inhalt des Profiling Warehouse.

Der Befehl „infacmd ps CreateWH“ verwendet die folgende Syntax:

```
CreateWH
<-DomainName|-dn> domain_name
[<-Gateway|-hp>] gateway_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-DsServiceName|-dsn> data_integration_service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps CreateWH“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_name	Optional. Verwenden Sie diese Option, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.inf“ veraltet sind. Geben Sie den Hostnamen und die Portnummer für den Gateway-Knoten in der Domäne ein. Verwenden Sie die folgende Syntax: gateway_hostname:port.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-DsServiceName -dsn	data_integration_service_name	Erforderlich. Name des Datenintegrationsdiensts.

# detectOrphanResults

Ermittelt Profilergebnisse im Profiling Warehouse, die nicht über ein zugehöriges Profil im Modellrepository verfügen. Wenn Sie ein Profil löschen, bevor Sie es öffnen, entfernt das Developer-Tool oder das Analyst-Tool das Profil und seine Metadaten aus dem Modellrepository. Die Aktion führt zu verwaisten Profilergebnissen im Profiling Warehouse. Um die verwaisten Profilergebnisse zu ermitteln, können Sie den Befehl `infacmd ps detectOrphanResults` ausführen. Um die Befehlsausgabe in einer Datei zu speichern, führen Sie den Befehl `infacmd ps detectOrphanResults > <filename> aus.`

Der Befehl „`infacmd ps detectOrphanResults`“ verwendet die folgende Syntax:

```
detectOrphanResults

<-DomainName|-dn> domain_name

[<-Gateway|-hp> gateway_name]

[<-NodeName|-nn>] node_name

<-UserName|-un> user_name

<-Password|-pd> Password

[<-SecurityDomain|-sdn> security_domain]

<-MrsServiceName|-msn> MRS_name

<-DsServiceName|-dsn> data_integration_service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd ps detectOrphanResults`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Der Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_name	Optional, wenn Sie den Befehl aus dem Informatica-Installationsverzeichnis \bin ausführen. Erforderlich, wenn Sie den Befehl von einem anderen Speicherort aus ausführen. Der Name des Gateway-Knotens. Verwenden Sie folgende Syntax: [Domain_Host]:[HTTP_Port]
-NodeName -nn	node_name	Erforderlich. Der Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	Passwort	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-MrsServiceName -msn	MRS_name	Erforderlich. Der Modellrepository-Dienstname.
-DsServiceName -dsn	data_integrations_service_name	Erforderlich. Der Datenintegrationsdienst-Name.

## DropWH

Entfernt den Inhalt des Profiling Warehouse.

Der Befehl „infacmd ps DropWH“ verwendet die folgende Syntax:

```
DropWH
```

```

<-DomainName|-dn> domain_name

[<-Gateway|-hp>] gateway_name]

<-UserName|-un> user_name

<-Password|-pd> Password

[<-SecurityDomain|-sdn> security_domain]

<-DsServiceName|-dsn> data_integration_service_name

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps DropWH“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_name	Optional. Verwenden Sie diese Option, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Geben Sie den Hostnamen und die Portnummer für den Gateway-Knoten in der Domäne ein. Verwenden Sie die folgende Syntax: gateway_hostname:port.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.



Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-DsServiceName -dsn	data_integration_service_name	Erforderlich. Name des Datenintegrationsdiensts.

## Execute

Führt ein Profil oder eine Scorecard aus.

Der Befehl „infacmd ps Execute“ verwendet die folgende Syntax:

```
Execute
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-NodeName|-nn> node_name]
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
<-ObjectType|-ot> object_type
<-ObjectPathAndName|-opn> MRS_object_path
[<-ProfileName|-pt> profile_task_name]
[<-wait|-w> true|false]
[<-ospn|-OsProfileName> os_profile_name]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps Execute“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-DsServiceName -dsn	data_inetgration_s ervice_name	Erforderlich. Name des Datenintegrationsdiensts.
-ObjectType -ot	object_type	Erforderlich. Geben Sie ein Profil oder eine Scorecard ein.
-ObjectPathandName -opn	MRS_object_path	Erforderlich. Verwenden Sie folgende Syntax:  ProjectName/FolderName/.../SubFolder_Name/ {ObjectName ProjectName/ObjectName}
-ProfileName -pt	profile_task_name	Optional. Name einer Profilaufgabe im Enterprise-Erkennungsprofil.
-Wait -w	true false	Optional. Wenn TRUE, wird vor der Rückkehr zur Eingabeaufforderung gewartet, bis der Befehl abgeschlossen ist. Wenn FALSE, wird zur Eingabeaufforderung zurückgekehrt, bevor der Befehl abgeschlossen ist. Standardwert ist „False“.
-ospn -OsProfileName	os_profile_name	Optional. Der Name des Betriebssystemprofils, wenn der Datenintegrationsdienst für die Verwendung von Betriebssystemprofilen eingerichtet ist.

## executeProfile

Führt ein Enterprise-Erkennungsprofil aus.

Der Befehl „infacmd ps executeProfile“ verwendet die folgende Syntax:

```
executeProfile
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-NodeName|-nn> node_name]
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
<-ObjectPathAndName|-opn> MRS_object_path
[<-WaitForModelExecToFinish|-w> true|false]
[<-ospn|-OsProfileName> os_profile_name]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps executeProfile“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-DsServiceName -dsn	data_inetgration_s ervice_name	Erforderlich. Name des Datenintegrationsdiensts.
-ObjectPathandName -opn	MRS_object_path	Erforderlich. Verwenden Sie folgende Syntax:  ProjectName/FolderName/.../SubFolder_Name/ {ObjectName ProjectName/ObjectName}
-WaitForModelExecToFinish -w	true false	Optional. Wenn TRUE, wird vor der Rückkehr zur Eingabeaufforderung gewartet, bis der Befehl abgeschlossen ist. Wenn FALSE, wird zur Eingabeaufforderung zurückgekehrt, bevor der Befehl abgeschlossen ist. Standardwert ist „False“.
-ospn -OsProfileName	os_profile_name	Optional. Der Name des Betriebssystemprofils, wenn der Datenintegrationsdienst für die Verwendung von Betriebssystemprofilen eingerichtet ist.

## getExecutionStatus

Ruft den Laufzeitstatus von Profilaufgaben in einem Enterprise-Erkennungsprofil ab.

Der Befehl „infacmd ps getExecutionStatus“ verwendet die folgende Syntax:

```
getExecutionStatus
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn> node_name]
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
<-ObjectType|-ot> object_type
<-ObjectPathAndName|-opn> MRS_object_path
<-ProfileTaskName|-pt> profile_task_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps getExecutionStatus“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-DsServiceName -dsn	data_integration_service_name	Erforderlich. Name des Datenintegrationsdiensts.
-ObjectType -ot	object_type	Erforderlich. Geben Sie ein Profil oder eine Scorecard ein.
-ObjectPathAndName -opn	MRS_object_path	Erforderlich. Verwenden Sie folgende Syntax: ProjectName/FolderName/.../SubFolder_Name/ {ObjectName ProjectName/ObjectName}
-ProfileTaskName -pt	profile_task_name	Optional. Name einer Profilaufgabe im Enterprise-Erkennungsprofil.

## getProfileExecutionStatus

Ruft den Laufzeitstatus eines Enterprise-Erkennungsprofils ab. Der Befehl listet auch alle Profilaufgaben im Enterprise-Erkennungsprofil sowie deren Laufzeitstatusangaben ab.

Der Befehl „infacmd ps getProfileExecutionStatus“ verwendet die folgende Syntax:

```
getProfileExecutionStatus
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn> node_name]
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
<-ObjectPathAndName|-opn> MRS_object_path
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps getProfileExecutionStatus“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.



Option	Argument	Beschreibung
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-DsServiceName -dsn	data_integration_s ervice_name	Erforderlich. Name des Datenintegrationsdiensts.
-ObjectPathAndName -opn	MRS_object_path	Erforderlich. Verwenden Sie folgende Syntax: ProjectName/FolderName/.../SubFolder_Name/ {ObjectName ProjectName/ObjectName}

## List

Listet Profile und Scorecards auf.

Der Befehl „infacmd ps List“ verwendet die folgende Syntax:

```
List
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn>] node_name
<-MrsServiceName|-msn> MRS_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-ObjectType|-ot>
<-FolderPath|-fp> full_folder_path
[<-Recursive|-r>]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps List“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:p ort gateway_host2:p ort...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ObjectType -ot	-	Erforderlich. Geben Sie ein Profil oder eine Scorecard ein.
-FolderPath -fp	full_folder_path	<p>Erforderlich. Geben Sie den Pfad des Ordners ein, der die aufzulistenden Objekte enthält.</p> <p>Verwenden Sie folgende Syntax:</p> <pre>Project_name/folder_name/./SubFolderName</pre>
-Recursive -r	-	Optional. Wendet den Befehl auf Objekte in dem von Ihnen angegebenen Ordner und seinen Unterordnern an.

# ListAllProfiles

Listet alle Profile in einem Enterprise-Erkennungsprofil auf.

Der Befehl `infacmd ps ListAllProfiles` verwendet die folgende Syntax:

```
ListAllProfiles  
  
<-DomainName|-dn> domain_name  
  
[<-Gateway|-hp> gateway_name]  
  
[<-NodeName|-nn>] node_name  
  
<-MrsServiceName|-msn> MRS_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-SecurityDomain|-sdn> security_domain]  
  
<-ProfilePathAndName|-pn>
```

In der folgenden Tabelle werden die Optionen und Argumente von `infacmd ps ListAllProfiles` beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/ Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ProfilePathAndName -pn	profile_path_and_name	Erforderlich. Geben Sie den Pfad zum Enterprise-Erkennungsprofil und dessen Namen ein.

## migrateProfileResults

Migriert Spaltenprofilergebnisse und Ergebnisse der Datendomänenerkennung aus Version 9.1.0, 9.5.0 oder 9.5.1.

Der Befehl „`infacmd ps migrateProfileResults`“ verwendet die folgende Syntax:

```

migrateProfileResults

<-DomainName|-dn> domain_name

[<-Gateway|-hp> gateway_name]

[<-NodeName|-nn> node_name]

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-MrsServiceName|-msn> MRS_name

<-DsServiceName|-dsn> data_integration_service_name

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps migrateProfileResults“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-DsServiceName -dsn	data_integration_service_name	Erforderlich. Name des Datenintegrationsdiensts.

## migrateScorecards

Migriert Scorecard-Ergebnisse aus Informatica 9.1.0 oder 9.5.0 bis 9.5.1.

Der Befehl „infacmd ps migrateScorecards“ verwendet die folgende Syntax:

```
migrateScorecards
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn> node_name]
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
<-migrateFrom|-mfr> migrate_from_release
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps migrateScorecards“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-DsServiceName -dsn	data_integration_service_name	Erforderlich. Name des Datenintegrationsdiensts.
-migrateFrom -mfr	migrate_from_release	<p>Erforderlich. Data Explorer-Version, von der die Migration erfolgt. Verwendet werden kann Version 9.1.0 oder 9.5.0.</p> <p>Wenn Sie Profile und Scorecards in Version 9.0, 9.0.1 oder 9.1.0 ausgeführt haben, geben Sie den Wert 9.1.0 ein. Wenn Sie Profile und Scorecards in Version 9.5.0 ausgeführt haben, geben Sie 9.5.0 als Wert ein.</p>

# Purge

Bereinigt Profil- oder Scorecard-Ergebnisse aus dem Profiling Warehouse. Der Befehl `infacmd ps Purge` löscht alle Profil- und Scorecard-Ergebnisse mit Ausnahme der Ergebnisse aus der aktuellen Profil- oder Scorecard-Ausführung.

Der Befehl „`infacmd ps Purge`“ verwendet die folgende Syntax:

```
Purge
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn>] node_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
<-ObjectType|-ot> object_type
<-ObjectPathAndName|-opn> MRS_object_path
[<-RetainDays|-rd> results_retain_days]
[<-ProjectFolderPath|-pf> project_folder_path]
[<-ProfileName|-pt> profile_task_name]
[<-Recursive|-r> recursive]
[<-PurgeAllResults|-pa> purge_all_results]
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd ps Purge`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Der Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_name	Optional, wenn Sie den Befehl aus dem Informatica-Installationsverzeichnis <code>\bin</code> ausführen. Erforderlich, wenn Sie den Befehl von einem anderen Speicherort aus ausführen. Der Name des Gateway-Knotens. Verwenden Sie folgende Syntax: <code>[Domain_Host]:[HTTP_Port]</code>
-NodeName -nn	node_name	Erforderlich. Der Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.



Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	Password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-MrsServiceName -msn	MRS_name	Erforderlich. Der Modellrepository-Dienstname.
-DsServiceName -dsn	data_integrations_service_name	Erforderlich. Der Datenintegrationsdienst-Name.
-ObjectType -ot	-	Erforderlich. Geben Sie ein Profil oder eine Scorecard ein.
-ObjectPathAndName -opn *	MRS_object_path	<p>Optional. Nicht mit ProjectFolderPath oder Recursive verwenden. Der Pfad zum Profil oder zur Scorecard im Modellrepository.</p> <p>Verwenden Sie folgende Syntax:</p> <pre>ProjectName/FolderName/.../{SubFolder_Name/ObjectName ProjectName/ObjectName}</pre>

Option	Argument	Beschreibung
-RetainDays -rd	results_retain_days	Optional. Gibt den Zeitraum für die Profil- und Scorecard-Ergebnisse an, die für die Speicherung im Profiling Warehouse geeignet sind. Der Datenintegrationsdienst löscht die übrigen Profil- und Scorecard-Ergebnisse.  Wenn Sie beispielsweise -rd 10 eingeben, werden die Ergebnisse vom aktuellen Tag und den letzten neun Tagen beibehalten und die übrigen Ergebnisse werden aus dem Profiling Warehouse gelöscht.
-ProjectFolderPath -pf *	project_folder_path	Optional. Nicht mit ObjectPathAndName oder ProfileTaskName verwenden.  Die Namen des Projekts und Ordners, in denen das Profil oder die Scorecard gespeichert ist. Verwenden Sie folgende Syntax:  ProjectName/FolderName
-ProfileName -pt *	profile_task_name	Optional. Der Name der Profilaufgabe, die Sie löschen möchten. Wenn ein Ordner nur ein Profil aufweist, können Sie nur die Option ProjectFolderPath verwenden, da ProjectFolderPath den Namen des Profils enthält, das die Profilaufgabe enthält. Wenn ein Ordner mehrere Profile in einem Ordner aufweist, müssen Sie für die Angabe des Profilenames die Optionen ProfileName und ProjectFolderPath kombinieren.
-Recursive -r	recursive	Optional. Nicht mit ObjectPathAndName verwenden.  Wendet den Befehl auf Objekte in dem von Ihnen angegebenen Ordner und seinen Unterordnern an.
-PurgeAllResults -pa	purge_all_results	Optional. Legen Sie diese Option fest, um alle Ergebnisse für das Profil- oder Scorecard-Objekt zu bereinigen.  Verwenden Sie die -recursive-Option, um den Befehl auf Profil- und Scorecard-Ergebnisse in dem angegebenen Ordner und seinen Unterordnern anzuwenden.
* Um den Befehl auszuführen, müssen Sie ObjectPathAndName oder ProjectFolderPath oder ProfileTaskName angeben.		

## purgeOrphanResults

Bereinigt die verwaisten Profilergebnisse aus dem Profiling Warehouse. Sie können diesen Befehl ausführen, nachdem Sie den Befehl „infacmd ps detectOrphanResults“ zum Erkennen der Profilergebnisse ausgeführt haben.

Der Befehl „infacmd ps purgeOrphanResults“ verwendet die folgende Syntax:

```
purgeOrphanResults
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn>] node_name
```

```

<-UserName|-un> user_name

<-Password|-pd> Password

[<-SecurityDomain|-sdn> security_domain]

<-MrsServiceName|-msn> MRS_name

<-DsServiceName|-dsn> data_integration_service_name

<-filePathName|-fpn> filePathName

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps purgeOrphanResults“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Der Name der Informatica-Domäne.  Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_name	Optional, wenn Sie den Befehl aus dem Informatica-Installationsverzeichnis \bin ausführen. Erforderlich, wenn Sie den Befehl von einem anderen Speicherort aus ausführen.  Der Name des Gateway-Knotens.  Verwenden Sie folgende Syntax:  [Domain_Host]:[HTTP_Port]
-NodeName -nn	node_name	Erforderlich. Der Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-MrsServiceName -msn	MRS_name	Erforderlich. Der Modellrepository-Dienstname.
-DsServiceName -dsn	data_integratio n_service_name	Erforderlich. Der Datenintegrationsdienst-Name.
-filePathName -fpn	filePathName	Erforderlich. Der Dateipfad mit dem Namen der Datei, die eine Liste mit Profil-IDs enthält. Die Profil-IDs werden den verwaisten Profilergebnissen zugeordnet, die bereinigt werden müssen.

## restoreProfilesAndScorecards

Stellt Profile und Scorecards aus einer früheren Version in der aktuellen Version wieder her.

Nach dem Upgrade und Drilldown auf die vorhandenen Profil- oder Scorecard-Ergebnisse werden Regelspalten möglicherweise nicht in den Drilldown-Ergebnissen angezeigt. Um Regelspalten in die Ergebnisse aufzunehmen, führen Sie den Befehl „`infacmd ps restoreProfilesAndScorecards`“ aus. Stellen Sie sicher, dass Sie ein Backup des Modellrepository-Inhalts erstellen, bevor Sie den Befehl ausführen.

Der Befehl `infacmd ps restoreProfilesAndScorecards` verwendet die folgende Syntax:

```
restoreProfilesAndScorecards
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn>] node_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
```

<-MrsServiceName|-msn> MRS\_name

<-DsServiceName|-dsn> data\_integration\_service\_name

In der folgenden Tabelle werden die Optionen und Argumente für `infacmd ps restoreProfilesAndScorecards` beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Der Name der Informatica-Domäne.  Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_name	Optional, wenn Sie den Befehl aus dem Informatica-Installationsverzeichnis \bin ausführen. Erforderlich, wenn Sie den Befehl von einem anderen Speicherort aus ausführen.  Der Name des Gateway-Knotens.  Verwenden Sie folgende Syntax:  [Domain_Host]:[HTTP_Port]
-NodeName -nn	node_name	Erforderlich. Der Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-MrsServiceName -msn	MRS_name	Erforderlich. Der Modellrepository-Dienstname.
-DsServiceName -dsn	data_integration_service_name	Erforderlich. Der Datenintegrationsdienst-Name..

## synchronizeProfile

Migriert dokumentierte, benutzerdefinierte und übernommene Primär- und Fremdschlüssel für alle Profile in einem Projekt der Version 9.1.0, 9.5.0 oder 9.5.1.

Der Befehl „`infacmd ps synchronizeProfile`“ verwendet die folgende Syntax:

```
synchronizeProfile
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn> node_name]
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
<-ProjectName|-pn> project_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps synchronizeProfile“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-DsServiceName -dsn	data_integration_service_name	Erforderlich. Name des Datenintegrationsdiensts.
-ProjectName -pn	project_name	Erforderlich. Projektname.



## KAPITEL 29

# infacmd pwx-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [CloseForceListener, 1037](#)
- [CloseListener, 1040](#)
- [CondenseLogger, 1043](#)
- [createdatamaps, 1046](#)
- [CreateListenerService, 1049](#)
- [CreateLoggerService, 1051](#)
- [DisplayAllLogger, 1056](#)
- [DisplayCPULogger, 1059](#)
- [DisplayEventsLogger, 1062](#)
- [DisplayMemoryLogger, 1065](#)
- [DisplayRecordsLogger, 1068](#)
- [displayStatsListener, 1071](#)
- [DisplayStatusLogger, 1074](#)
- [FileSwitchLogger, 1077](#)
- [ListTaskListener, 1080](#)
- [ShutDownLogger, 1083](#)
- [StopTaskListener, 1086](#)
- [UpgradeModels, 1089](#)
- [UpdateListenerService, 1092](#)
- [UpdateLoggerService, 1096](#)

## CloseForceListener

Erzwingt den Abbruch lang andauernder Unteraufgaben auf dem PowerExchange-Listenerdienst und stoppt den Listenerdienst.

Wenn Sie den Befehl `infacmd pwx CloseForceListener` verwenden, schließt PowerExchange die folgenden Aktionen ab:

1. Prüfen, ob alle Unteraufgaben im Listenerdienst aktiv sind.

2. Sind aktive Unteraufgaben vorhanden, wird die Anzahl der Unteraufgaben über einen Zeitraum von 30 Sekunden im Sekundentakt abgefragt.
3. Während dieses Zeitraums wird jede Unteraufgabe angehalten, die auf eine TCP/IP-Netzwerkeingabe wartet.
4. Abbrechen aller verbleibenden aktiven Unteraufgaben.
5. Anhalten des Listenerdiensts.

Der Befehl „infacmd pwx CloseForceListener“ verwendet die folgende Syntax:

```
CloseForceListener
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx CloseForceListener“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Listenerdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänenamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-OSUser -oun	OS_user_name	<p>Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem.</p> <p>Aktivieren Sie Betriebssystemsicherheit wie folgt:</p> <ul style="list-style-type: none"> <li>- Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren.</li> <li>- Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.</li> </ul> <p>Weitere Informationen finden Sie im <i>PowerExchange-Referenzhandbuch</i>.</p>
-OSPassword -oup	OS_password	<p>Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem.</p> <p>Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.</p>
-OSEPassword -ouep	OS_epassword	<p>Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem.</p> <p>Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.</p>

## CloseListener

Hält den PowerExchange-Listenerdienst an, wenn alle ausstehenden Unteraufgaben im Listenerdienst abgeschlossen sind.

**Hinweis:** Befinden sich im Listenerdienst lang andauernde Unteraufgaben, verwenden Sie den Befehl „infacmd pwx closeforceListener“, um den Abbruch aller Unteraufgaben zu erzwingen und den Listenerdienst anzuhalten.

Der Befehl „infacmd pwx CloseListener“ verwendet die folgende Syntax:

```
CloseListener

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-OSUser|-oun> OS_user_name]

[<-OSPassword|-oup> OS_password]

[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx CloseListener“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Listenerdiensts.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-OSUser -oun	OS_user_name	<p>Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem.</p> <p>Aktivieren Sie Betriebssystemsicherheit wie folgt:</p> <ul style="list-style-type: none"> <li>- Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren.</li> <li>- Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.</li> </ul>

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem.  Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem.  Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.

## CondenseLogger

Startet einen weiteren Logging-Zyklus, bevor die Wartezeit für das Starten eines anderen Zyklus verstrichen ist, wenn der PowerExchange-Protokollierungsdienst im fortlaufenden Modus ausgeführt wird. Legen Sie die Wartezeit im Parameter NO\_DATA\_WAIT der Konfigurationsdatei „pwxocl.cfg“ fest.

Der Befehl „infacmd pwx CondenseLogger“ verwendet die folgende Syntax:

```
CondenseLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx CondenseLogger“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Protokollierungsdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.



Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	<p>Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.</p>
-OSUser -oun	OS_user_name	<p>Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem.</p> <p>Aktivieren Sie Betriebssystemsicherheit wie folgt:</p> <ul style="list-style-type: none"> <li>- Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren.</li> <li>- Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.</li> </ul>

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	<p>Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem.</p> <p>Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.</p>
-OSEPassword -ouep	OS_epassword	<p>Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem.</p> <p>Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.</p>

## createdatamaps

Erstellt Datenzuordnungen für Massendatenbewegungsoperationen.

Verwenden Sie den Befehl `createdatamaps` zum Generieren von Datenzuordnungen für IMS-, SEQ- und VSAM-Datenquellen über die Befehlszeile. Dieser Befehl bietet in bestimmten Fällen eine Alternative zur Verwendung des PowerExchange Navigator und ermöglicht Ihnen, Datenzuordnungen nicht interaktiv zu generieren oder neu zu generieren.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, erhöhen Sie den verfügbaren Speicher für „infacmd“. Um den Systemspeicher zu erhöhen, legen Sie den Wert „-Xmx“ in der Umgebungsvariable `ICMD_JAVA_OPTS` fest. Weitere Informationen hierzu finden Sie unter [“ICMD\\_JAVA\\_OPTS” auf Seite 45](#).

Der Befehl „`infacmd pwx createdatamaps`“ verwendet die folgende Syntax:

```
createdatamaps
[<-pwxLocation|-loc> pwx_location]
[<-pwxUserName|-pun> pwx_user_name]
[<-pwxPassword|-ppd> pwx_password]
[<-pwxEncryptedPassword|-epwd> pwx_encrypted_password]
[<-datamapOutputDir|-dod> datamap_output_directory]
[<-replace|-r> replace_existing_datamaps]
<-controlFile|-cf> file_path_for_control_file
[<-logFile|-lf> file_path_for_log_file]
[<-verbosity|-v> logging_verbosity]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx createdatamaps“ beschrieben:

Option	Argument	Beschreibung
-pwxLocation -loc	pwx_location	Optional. Der Speicherort der Datenquelle, wie in einer NODE-Anweisung in der dbmover-Konfigurationsdatei von PowerExchange angegeben. Wenn pwxLocation nicht angegeben ist, greift das Dienstprogramm createdatamaps auf das Copybook und die DBD-Metadaten im lokalen Dateisystem zu.  Wenn Sie die Steuerungsdatei zum Auffinden von Datensatz-IDs konfigurieren, ist pwxLocation erforderlich.
-pwxUserName -pun	pwx_user_name	Optional. Die Benutzer-ID für die Verbindung zum PowerExchange Listener, wenn pwxLocation angegeben ist.
-pwxPassword -ppd	pwx_password	Optional. Passwort für eine Verbindung zum PowerExchange Listener, wenn pwxLocation angegeben ist.  Anstelle eines Passworts können Sie eine gültige PowerExchange Passphrase eingeben. Passphrasen für den Zugriff auf einen PowerExchange Listener unter z/OS kann von 9 bis 128 Zeichen lang sein und folgende Zeichen enthalten: <ul style="list-style-type: none"> <li>- Groß- und Kleinbuchstaben</li> <li>- Die Zahlen 0 bis 9</li> <li>- Leerzeichen</li> <li>- Die folgenden Sonderzeichen: ' - ; # \ , . / ! % &amp; * ( ) _ + { } : @   &lt; &gt; ?</li> </ul> <p><b>Hinweis:</b> Das erste Zeichen ist ein Apostroph.</p> <p>Passphrasen dürfen keine einfachen Anführungszeichen ('), doppelten Anführungszeichen (") oder Währungssymbole enthalten.</p> <p>Wenn eine Passphrase Leerzeichen enthält, müssen Sie sie in doppelte Anführungszeichen setzen. Beispiel: „Das ist eine Beispiel-Passphrase“. Wenn eine Passphrase Sonderzeichen enthält, müssen Sie sie in dreifache doppelte Anführungszeichen (""") setzen. Beispiel: """"Diese Passphrase enthält Sonderzeichen. % &amp; *.""".</p> <p>Wenn eine Passphrase nur alphanumerische Zeichen ohne Leerzeichen enthält, können Sie sie ohne Delimiter eingeben.</p> <p><b>Hinweis:</b> Auf z/OS kann eine gültige RACF-Passphrase bis zu 100 Zeichen umfassen. PowerExchange schneidet Passphrases mit mehr als 100 Zeichen ab, wenn diese zur Validierung an RACF übergeben werden.</p> <p>Stellen Sie vor der Verwendung von Passphrasen sicher, dass der PowerExchange-Listenerdienst im DBMOVER-Mitglied mit der Sicherheitseinstellung SECURITY=(1,N) oder höher ausgeführt wird. Weitere Informationen finden Sie unter „SECURITY-Anweisung“ im <i>PowerExchange-Referenzhandbuch</i>.</p>

Option	Argument	Beschreibung
-pwxEncryptedPassword -epwd	pwx_encrypted_password	Optional. Verschlüsseltes Passwort für eine Verbindung zum PowerExchange Listener, wenn pwxLocation angegeben ist. Wenn der PowerExchange Listener auf einem z/OS- oder i5/OS-System ausgeführt wird, können Sie eine verschlüsselte PowerExchange-Passphrase anstelle eines verschlüsselten Passworts eingeben. Verschlüsseln Sie keine Passphrase, die ungültige Zeichen wie z. B. doppelte Anführungszeichen, einzelne Anführungszeichen oder Währungssymbole enthält.
-datamapOutputDir -dod	datamap_output_directory	Optional. Das lokale Dateiverzeichnis, in das die Ausgabe-Datenzuordnungen geschrieben werden sollen. Standardwert ist das aktuelle Arbeitsverzeichnis.
-replace -r	replace_existing_datamaps	Optional. Gibt an, ob vorhandene Datenzuordnungen ersetzt werden sollen. Im Fall von replace=Y werden alle Datenzuordnungen in datamap_output_directory ersetzt, die denselben Namen als Datenzuordnungen haben, die Sie erstellen. Im Fall von replace=N wird die Erstellung einer Datenzuordnung bersprungen, falls eine Datenzuordnung mit demselben Namen bereits in datamap_output_directory existiert. Standardwert ist „N“.
-controlFile -cf	file_path_for_control_file	Erforderlich. Pfad und Dateiname der Steuerdatei, die die Datenzuordnungs-Erzeugung steuert.
-logFile -lf	file_path_for_log_file	Optional. Pfad und Dateiname der Ausgabeprotokolldatei. Standardwert ist „STDOUT“.
-verbosity -v	logging_verbosity	Optional. Ausführlichkeit für Protokolldateien. Standardwert ist „INFO“. Gültige Werte: - DEBUG. Detailliertere Protokollierung. Zeigt möglicherweise Stapelüberwachungen an. - INFO. Informationsmeldungen. - WARN. Gibt ein potenzielles Problem an. - ERROR. Gibt einen Fehler an. Die Verarbeitung wird fortgesetzt. - FATAL. Gibt eine schwerwiegende Fehlerbedingung an. Der Prozess wird beendet.

Der PowerExchange-Knotenname und die Anmeldedaten sind optional. Wenn Sie die Option „pwxLocation“ nicht einbeziehen, greift der Befehl direkt auf das lokale Dateisystem zu, um Metadaten zu lesen. In diesem Fall muss PowerExchange nicht auf dem Computer installiert sein, auf dem Sie createdatamaps ausführen.

Weitere Informationen zum Befehl „createdatamaps“ finden Sie im *PowerExchange Utilities-Handbuch*.

# CreateListenerService

Erstellt einen PowerExchange-Listenerdienst in einer Domäne. Standardmäßig wird der Listenerdienst bei seiner Erstellung deaktiviert. Führen Sie den Befehl „infacmd isp EnableService“ aus, um den Dienst zu aktivieren.

Der Befehl „infacmd pwx CreateListenerService“ verwendet die folgende Syntax:

```
CreateListenerService

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

[<-LicenseName|-ln> license_name]

[<-BackupNode|-bn> backup_node]

<-StartParameters|-sp> start_parameters

<-SvcPort|-vp> service_port
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx CreateListenerService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn -DomainName nicht angegeben wurde. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Listenerdiensts. Bei diesem Namen wird die Groß-/Kleinschreibung nicht beachtet. Der Name darf nicht mehr als 128 Zeichen umfassen und keine Wagenrückläufe, Tabulatoren, Leerzeichen oder die folgenden Zeichen enthalten:  / * ? < > "
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Listenerdienst ausgeführt werden soll.
-LicenseName -ln	license_name	Optional. Lizenz zur Zuweisung zum Dienst. Wenn Sie jetzt keine Lizenz auswählen, können Sie dem Dienst später eine Lizenz zuweisen. Dies ist erforderlich, bevor Sie den Dienst aktivieren können.
-BackupNode -bn	backup_node	Optional. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, wird mit dieser Option der Name des Backup-Knotens angegeben.

Option	Argument	Beschreibung
-StartParameters -sp	start_parameters	<p>Parameter, die beim Starten des Listenerdiensts einbezogen werden müssen. Trennen Sie die Parameter durch Leerzeichen. Der Parameter <i>node_name</i> ist erforderlich.</p> <p>Sie können die folgenden Parameter einbeziehen:</p> <ul style="list-style-type: none"> <li>- <i>node_name</i> Erforderlich. Knotenname, der den Listenerdienst identifiziert. Dieser Name muss mit dem Namen in der LISTENER-Anweisung in der Konfigurationsdatei DBMOVER übereinstimmen.</li> <li>- <i>config=directory</i> Optional. Gibt den vollständigen Pfad und Dateinamen für die Konfigurationsdatei „dbmover.cfg“ an, die Sie anstelle der Standarddatei „dbmover.cfg“ verwenden möchten. Diese alternative Konfigurationsdatei hat Vorrang vor jeder anderen alternativen Konfigurationsdatei, die Sie in der Umgebungsvariable PWX_CONFIG angeben.</li> <li>- <i>license=directory/license_key_file</i> Optional. Gibt den vollständigen Pfad und Dateinamen für eine Lizenzschlüsseldatei an, die Sie anstelle der Standarddatei license.key verwenden möchten. Diese alternative Lizenzschlüsseldatei und die Standarddatei dürfen nicht denselben Namen und denselben Pfad haben. Entweder Name oder Pfad muss unterschiedlich sein. Diese alternative Lizenzschlüsseldatei hat Vorrang vor jeder anderen alternativen Lizenzschlüsseldatei, die Sie in der Umgebungsvariable PWX_LICENSE angeben.</li> </ul> <p><b>Hinweis:</b> In den Konfigurations- und Lizenzparametern müssen Sie den vollständigen Pfad nur dann angeben, wenn die Datei sich <i>nicht</i> im Installationsverzeichnis befindet. Schließen Sie Pfad- und Dateinamen, die Leerzeichen enthalten, in Anführungszeichen ein.</p>
-SvcPort -vp	service_port	Erforderlich. Port des Listenerdiensts für die Reaktion auf Befehle vom Dienstmanager.

## CreateLoggerService

Erstellt einen PowerExchange-Protokollierungsdienst in einer Domäne. Standardmäßig wird der Protokollierungsdienst bei seiner Erstellung deaktiviert. Führen Sie den Befehl „infacmd isp EnableService“ aus, um den Dienst zu aktivieren.

Der Befehl „infacmd pwx CreateLoggerService“ verwendet die folgende Syntax:

```
CreateLoggerService
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
[<-SecurityDomain|-sdn> security_domain]
```

```
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

[<-LicenseName|-ln> license_name]

[<-BackupNode|-bn> backup_node]

[<-StartParameters|-sp> start_parameters>]

<-SvcPort|-vp> service_port
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx CreateLoggerService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.



Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Optional. Wenn -DomainName nicht angegeben wurde. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Protokollierungsdiensts. Bei diesem Namen wird die Groß-/Kleinschreibung nicht beachtet. Der Name darf nicht mehr als 128 Zeichen umfassen und keine Wagenrückläufe, Tabulatoren, Leerzeichen oder die folgenden Zeichen enthalten: / * ? < > "
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Protokollierungsdienst ausgeführt werden soll.
-LicenseName -ln	license_name	Optional. Lizenz zur Zuweisung zum Dienst. Wenn Sie jetzt keine Lizenz auswählen, können Sie dem Dienst später eine Lizenz zuweisen. Dies ist erforderlich, bevor Sie den Dienst aktivieren können.
-BackupNode -bn	backup_node	Optional. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, wird mit dieser Option der Name des Backup-Knotens angegeben.

Option	Argument	Beschreibung
-StartParameters -sp	start_parameters	<p>Optional. Parameter, die beim Starten des Protokollierungsdiensts einbezogen werden müssen. Trennen Sie die Parameter durch Leerzeichen.</p> <p>Sie können die folgenden Parameter einbeziehen:</p> <ul style="list-style-type: none"> <li>- coldstart={Y N} Gibt an, ob der Protokollierungsdienst kalt oder warm gestartet wird. Geben Sie Y für einen Kaltstart des Protokollierungsdiensts ein. Wenn die CDCT-Datei Protokolldatensätze enthält, löscht der Protokollierungsdienst diese Datensätze. Geben Sie N ein, um den Protokollierungsdienst ab dem Neustartpunkt warm zu starten, der in der CDCT-Datei angegeben ist. Standardwert ist „N“.</li> <li>- config=directory/pwx_config_file Gibt den vollständigen Pfad und Dateinamen für die Konfigurationsdatei „dbmover.cfg“ an, die Sie anstelle der Standarddatei „dbmover.cfg“ verwenden möchten. Diese alternative Konfigurationsdatei hat Vorrang vor jeder anderen alternativen Konfigurationsdatei, die Sie in der Umgebungsvariable PWX_CONFIG angeben.</li> <li>- cs=directory/pwxlogger_config_file Gibt den Pfad und Dateinamen für die Konfigurationsdatei des Protokollierungsdiensts an. Sie können auch den cs-Parameter verwenden, um eine Protokollierungsdienst-Konfigurationsdatei anzugeben, die die Standarddatei pwxcl.cfg überschreibt. Diese Überschreibungsdatei und die Standarddatei dürfen nicht denselben Namen und denselben Pfad haben. Entweder Name oder Pfad muss unterschiedlich sein.</li> <li>- encryptpwd=encrypted_password Ein Passwort im verschlüsselten Format zum Aktivieren der Verschlüsselung von Protokolldateien der PowerExchange-Protokollierung. Mit diesem Passwort kann die PowerExchange-Protokollierung einen eindeutigen Verschlüsselungsschlüssel für jede Protokolldatei der Protokollierung erzeugen. Das Passwort wird in der CDCT-Datei im verschlüsselten Format gespeichert. Aus Sicherheitsgründen wird das Passwort weder in CDCT-Sicherungsdateien gespeichert noch in den CDCT-Berichten angezeigt, die mit dem PowerExchange-Dienstprogramm PWXUCDCT erzeugt werden können. Bei Angabe dieses Parameters müssen Sie auch coldstart=y angeben. Wenn Sie diesen Parameter und den Parameter ENCRYPTPWD in der Konfigurationsdatei (pwxcl.cfg) der PowerExchange-Protokollierung angeben, hat der Parameter in der Konfigurationsdatei Vorrang. Wenn Sie diesen Parameter und den Parameter ENCRYPTPWD in der Konfigurationsdatei der PowerExchange-Protokollierung angeben, tritt ein Fehler auf. Sie können den AES-Algorithmus festlegen, um ihn zum Verschlüsseln der Protokolldatei im Parameter ENCRYPTOPT der Datei „pwxcl.cfg“ zu verwenden. Standardwert ist AES128.</li> </ul>

Option	Argument	Beschreibung
		<p><b>Tipp:</b> Zur Sicherheitsoptimierung empfiehlt Informatica, das Verschlüsselungspasswort beim Kaltstart der PowerExchange-Protokollierung und nicht in der Konfigurationsdatei „pwxccl.cfg“ anzugeben. Mit dieser Vorgehensweise verringern Sie aus folgenden Gründen das Risiko eines böswilligen Zugriffs auf das Verschlüsselungspasswort: 1) Das Verschlüsselungspasswort ist nicht in der Datei „pwxccl.cfg“ gespeichert. 2) Sie können das Passwort nach einem erfolgreichen Kaltstart aus der Befehlszeile löschen. Wenn Sie das Verschlüsselungspasswort für einen Kaltstart angeben und die CDCT-Datei dann zu einem späteren Zeitpunkt wiederherstellen müssen, müssen Sie dasselbe Verschlüsselungspasswort im Befehl RESTORE_CDCT des Dienstprogramms PWXUCDCT eingeben.</p> <p>Um die Protokolldateien der PowerExchange-Protokollierung <i>nicht</i> zu verschlüsseln, geben Sie kein Verschlüsselungspasswort ein.</p> <ul style="list-style-type: none"> <li>- <code>license=directory/license_key_file</code> Gibt den vollständigen Pfad und Dateinamen für eine Lizenzschlüsseldatei an, die Sie anstelle der Standarddatei <code>license.key</code> verwenden möchten. Diese alternative Lizenzschlüsseldatei und die Standarddatei dürfen nicht denselben Namen und denselben Pfad haben. Entweder Name oder Pfad muss unterschiedlich sein. Diese alternative Lizenzschlüsseldatei hat Vorrang vor jeder anderen alternativen Lizenzschlüsseldatei, die Sie in der Umgebungsvariable <code>PWX_LICENSE</code> angeben.</li> <li>- <code>specialstart={Y N}</code> Gibt an, ob ein Sonderstart der PowerExchange-Protokollierung durchgeführt werden soll. Ein Sonderstart startet die Verarbeitung der PowerExchange-Erfassung an dem Punkt im Änderungsstrom, den Sie in der Datei „pwxccl.cfg“ angeben. Dieser Startpunkt überschreibt den Neustartpunkt aus der CDCT-Datei für die PowerExchange-Protokollierungsausführung. Bei einem Sonderstart wird kein Inhalt aus der CDCT-Datei gelöscht.</li> </ul> <p>Verwenden Sie diesen Parameter zum Überspringen problematischer Stellen in den Quellprotokollen, ohne dabei erfasste Daten zu verlieren. Verwenden Sie einen Sonderstart beispielsweise in folgenden Situationen:</p> <ul style="list-style-type: none"> <li>- Sie möchten nicht, dass die PowerExchange-Protokollierung eine Aktualisierung eines Oracle-Katalogs erfasst. Stoppen Sie in diesem Fall die PowerExchange-Protokollierung vor der Aktualisierung. Erzeugen Sie nach Abschluss der Aktualisierung eine neue Sequenz und starten Sie Token für die PowerExchange-Protokollierung basierend auf dem Post-Upgrade-SCN neu. Geben Sie diese Token-Werte in den Parametern <code>SEQUENCE_TOKEN</code> und <code>RESTART_TOKEN</code> in der Datei „pwxccl.cfg“ ein und führen Sie dann einen Sonderstart der PowerExchange-Protokollierung durch.</li> <li>- Sie möchten nicht, dass von der PowerExchange-Protokollierung alte, nicht verfügbare Protokolle erneut verarbeitet werden, die durch ausstehende Arbeitseinheiten verursacht wurden, die nicht zu CDC gehören. Stoppen Sie in diesem Fall die PowerExchange-Protokollierung. Bearbeiten Sie den Wert <code>RESTART_TOKEN</code>, um den SCN des frühesten verfügbaren Protokolls widerzuspiegeln, und</li> </ul>

Option	Argument	Beschreibung
		<p>führen Sie dann einen Sonderstart durch. Wenn alle ausstehenden Arbeitseinheiten, die vor diesem Neustartpunkt gestartet wurden, zu CDC gehören, gehen unter Umständen Daten verloren.</p> <p>Gültige Werte:</p> <ul style="list-style-type: none"> <li>- Y. Führen Sie einen Sonderstart der PowerExchange-Protokollierung ab dem Punkt im Änderungsstrom durch, der von den Parameterwerten SEQUENCE_TOKEN und RESTART_TOKEN in der Konfigurationsdatei „pwxcl.cfg“ definiert wird. Sie müssen gültige Token-Werte in der Datei „pwxcl.cfg“ angeben, um einen Sonderstart durchzuführen. Diese Token-Werte überschreiben die Token-Werte aus der CDCT-Datei. Stellen Sie sicher, dass der Wert SEQUENCE_TOKEN in der Datei „pwxcl.cfg“ größer oder gleich dem aktuellen Sequenz-Token in der CDCT-Datei ist. Geben Sie den Parameter coldstart=Y nicht noch zusätzlich an. Wenn Sie den Parameter coldstart=Y angeben, hat dieser Parameter Vorrang.</li> <li>- N. Führen Sie keinen Sonderstart durch. Führen Sie einen Kalt- oder Warmstart, wie vom coldstart-Parameter angegeben, durch.</li> </ul> <p>Standardwert ist „N“.</p> <p><b>Hinweis:</b> Der vollständige Pfad muss in den Konfigurations-, cs- und Lizenzparametern nur angegeben werden, wenn sich die Datei <i>nicht</i> im Installationsverzeichnis befindet. Schließen Sie Pfad- und Dateinamen, die Leerzeichen enthalten, in Anführungszeichen ein.</p>
-SvcPort -vp	service_port	Optional. Port des Protokollierungsdiensts für die Reaktion auf Befehle vom Dienstmanager.

## DisplayAllLogger

Zeigt sortiert nach Befehl alle Nachrichten an, die von den Anzeigebefehlen des anderen PowerExchange-Protokollierungsdiensts erzeugt werden können.

Der Befehl „infacmd pwx DisplayAllLogger“ zeigt die konsolidierte Ausgabe für die folgenden Befehle an:

- DisplayCPULogger
- DisplayEventsLogger
- DisplayMemoryLogger
- DisplayRecordsLogger
- DisplayStatusLogger

Der Befehl „infacmd pwx DisplayAllLogger“ verwendet die folgende Syntax:

```
DisplayAllLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
```

```

[<-Password|-pd> password]

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-OSUser|-oun> OS_user_name]

[<-OSPassword|-oup> OS_password]

[<-OSEPassword|-ouep> OS_epassword]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx DisplayAllLogger“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Protokollierungsdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	<p>Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.</p>
-OSUser -oun	OS_user_name	<p>Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem.</p> <p>Aktivieren Sie Betriebssystemsicherheit wie folgt:</p> <ul style="list-style-type: none"> <li>- Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren.</li> <li>- Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.</li> </ul>

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	<p>Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem.</p> <p>Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.</p>
-OSEPassword -ouep	OS_epassword	<p>Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem.</p> <p>Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.</p>

## DisplayCPULogger

Zeigt die CPU-Zeit in Mikrosekunden an, die vom PowerExchange-Protokollierungsdienst für jede Phase der Verarbeitung während des aktuellen Logging-Zyklus benötigt wird. Enthält außerdem die CPU-Gesamtzeit für die gesamte Protokollierungsdienst-Verarbeitung.

Mit dem Befehl „infacmd pwx DisplayCPULogger“ kann beispielsweise die CPU-Zeit angegeben werden, die vom Protokollierungsdienst zum Abschließen der folgenden Aktionen benötigt wird:

- Lesen von Quelldaten
- Schreiben von Daten in die Protokolldateien des Protokollierungsdiensts
- Durchführen von Dateiwechseln
- Durchführen weiterer Verarbeitungsaufgaben, wie z. B. das Initialisieren und Verarbeiten von Befehlen

Der Befehl „infacmd pwx DisplayCPULogger“ verwendet die folgende Syntax:

```
DisplayCPULogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx DisplayCPULogger“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Protokollierungsdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.



Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	<p>Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.</p>
-OSUser -oun	OS_user_name	<p>Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem.</p> <p>Aktivieren Sie Betriebssystemsicherheit wie folgt:</p> <ul style="list-style-type: none"> <li>- Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren.</li> <li>- Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.</li> </ul>

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem.  Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem.  Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.

## DisplayEventsLogger

Zeigt Ereignisse an, auf die die Controller-, Command Handler- und Writer-Aufgaben für den PowerExchange-Protokollierungsdienst warten. Gibt außerdem an, ob der Writer Daten verarbeitet oder im Ruhemodus ausgeführt wird und auf das Auftreten eines Ereignisses oder Timeouts wartet.

Der Befehl „`infacmd pwx DisplayEventsLogger`“ verwendet die folgende Syntax:

```
DisplayEventsLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx DisplayEventsLogger“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Protokollierungsdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	<p>Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.</p>
-OSUser -oun	OS_user_name	<p>Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem.</p> <p>Aktivieren Sie Betriebssystemsicherheit wie folgt:</p> <ul style="list-style-type: none"> <li>- Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren.</li> <li>- Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.</li> </ul>

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem.  Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem.  Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.

## DisplayMemoryLogger

Zeigt die Speichernutzung (in Byte) für jede Aufgabe und Unteraufgabe im PowerExchange-Protokollierungsdienst mit Gesamtsummen für den gesamten Protokollierungsdienst-Prozess an.

PowerExchange gibt die Speichernutzung für folgende Kategorien an:

- Application Speicher, der von der Protokollierungsdienst-Anwendung zur eigenen Nutzung benötigt wird.
- Gesamt. Gesamter für die Protokollierungsdienst-Anwendung und den zugehörigen Header-Overhead verwendeter Speicher. Dieser Wert variiert, da PowerExchange während der Protokollierungsdienst-Verarbeitung Speicher zuweist und freigibt.
- Maximal. Die größte für die Kategorie „Gesamt“ aufgezeichnete Speichermenge bis zu dem Zeitpunkt, an dem dieser Befehl ausgeführt wird.

Der Befehl „`infacmd pwx DisplayMemoryLogger`“ verwendet die folgende Syntax:

```
DisplayMemoryLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx DisplayMemoryLogger“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Protokollierungsdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	<p>Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.</p>
-OSUser -oun	OS_user_name	<p>Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem.</p> <p>Aktivieren Sie Betriebssystemsicherheit wie folgt:</p> <ul style="list-style-type: none"> <li>- Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren.</li> <li>- Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.</li> </ul>

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem.  Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem.  Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.

## DisplayRecordsLogger

Zeigt die Anzahl der Änderungsdatensätze an, die vom PowerExchange-Protokollierungsdienst während des aktuellen Verarbeitungszyklus verarbeitet wurden. Wenn der Protokollierungsdienst während des aktuellen Zyklus keine Änderungen erhalten hat, wird die Anzahl der Änderungsdatensätze für den aktuellen Satz an Protokolldateien des Protokollierungsdiensts angezeigt.

Der Befehl „`infacmd pwx DisplayRecordsLogger`“ zeigt die Anzahl an Datensätzen für jeden verarbeiteten Typ der Änderungsdatensätze sowie für die Gesamtzahl der verarbeiteten Datensätze an. Zu den Änderungsdatensatztypen gehören: Delete, Insert, Update und Commit.

Je nachdem, ob der Befehl Zähler für den aktuellen Zyklus oder die aktuellen Logdateien anzeigt, enthält die Ausgabe alle oder bestimmte der folgenden Informationstypen:

- **Zyklus.** Anzahl der Änderungsdatensätze für den aktuellen Protokollierungsdienst-Verarbeitungszyklus. Der Protokollierungsdienst setzt diese Anzahl auf „null“ zurück, wenn der im Parameter NO\_DATA\_WAIT2 der Datei „`pwxcccl.cfg`“ angegebene Wartezeitraum abläuft oder wenn keine Änderungsdaten empfangen wurden.
- **Datei.** Anzahl der Änderungsdatensätze für den aktuellen Satz an PowerExchange-Logdateien. Der Protokollierungsdienst setzt diese Anzahl auf „null“ zurück, wenn ein Dateiwechsel stattfindet.
- **Gesamt.** Anzahl der Änderungsdatensätze, die der Protokollierungsdienst seit seinem Start erhalten hat. PowerExchange setzt diese Anzahl nicht auf Null zurück.

Der Befehl „`infacmd pwx DisplayRecordsLogger`“ verwendet die folgende Syntax:

```
DisplayRecordsLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
[<-ServiceName|-sn> service_name
```



```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-OSUser|-oun> OS_user_name]

[<-OSPassword|-oup> OS_password]

[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx DisplayRecordsLogger“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Protokollierungsdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	<p>Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.</p>
-OSUser -oun	OS_user_name	<p>Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem.</p> <p>Aktivieren Sie Betriebssystemsicherheit wie folgt:</p> <ul style="list-style-type: none"> <li>- Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren.</li> <li>- Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.</li> </ul>

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem.  Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem.  Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.

## displayStatsListener

Zeigt die Überwachungsstatistik für einen PowerExchange-Listener unter Linux, UNIX oder Windows an, den der PowerExchange-Listenerdienst verwaltet. Zeigt außerdem Statistiken für die Client-Aufgaben und Quell- oder Zielverbindungen, die dem Listener zugeordnet sind.

Der Befehl kann die folgenden Arten von Statistiken drucken, je nachdem, welche Option Sie für „-type“ angeben:

- Zusammenfassung der PowerExchange-Listener-Statistiken über Arbeitsspeichernutzung, CPU-Verarbeitungszeit und Aktivität für Clientanfragen. Diese Statistiken enthalten die Anzahl von Client-Aufgaben, Verbindungen, gesendeten und empfangenen Nachrichten sowie gesendeten und empfangenen Datenbytes.
- Nachrichten- und Datenmengen, die Client-Aufgaben für Client-Anfragen gesendet und empfangen haben, nach Aufgaben-ID und Zugriffsmethode. Die Nachrichten- und Datenmengen sind Summen zu dem Zeitpunkt, zu dem die Statistiken generiert werden.
- Informationen über die aktiven Aufgaben, die unter dem Listener zur Verarbeitung von Client-Anfragen ausgeführt werden. Diese Statistiken enthalten die Aufgaben-Startzeit, die CPU-Verarbeitungszeit, die Zugriffsmethode, den Lese- oder Schreibmodus und zugeordnete Prozess- und Sitzungs-IDs. Enthält außerdem die Portnummer und die IP-Adresse des Clients, der die Anfrage an den PowerExchange-Listener ausgegeben hat.

**Wichtig:** Damit PowerExchange die Überwachungsstatistiken vom PowerExchange-Listener erfassen kann, müssen Sie den Parameter MONITOR in der Anweisung STATS in der DBMOVER-Konfigurationsdatei angeben, in der der Listener ausgeführt wird.

Der Befehl „`infacmd pwx displayStatsListener`“ verwendet die folgende Syntax:

```
displayStatsListener
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
```

```
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> domain_host1:port domain_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
[<-Type|-tp> report_type]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx displayStatsListener“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Listenerdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	<p>Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.</p>
-OSUser -oun	OS_user_name	<p>Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem.</p> <p>Aktivieren Sie Betriebssystemsicherheit wie folgt:</p> <ul style="list-style-type: none"> <li>- Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren.</li> <li>- Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.</li> </ul>
-OSPassword -oup	OS_password	<p>Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem.</p> <p>Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.</p>

Option	Argument	Beschreibung
-OSEPassword -ouep	OS_epassword	<p>Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpassword festlegen. Verschlüsseltes Passwort für das Betriebssystem.</p> <p>Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.</p>
-type -tp	report_type	<p>Optional. Der Typ von Überwachungsstatistiken zum Berichten für den PowerExchange-Listener und dessen Client-Aufgaben und Verbindungen. Für report_type muss einer der folgenden Werte angegeben werden:</p> <ul style="list-style-type: none"> <li>- Listener. Berichtet für einen bestimmten PowerExchange-Listener über Speichernutzung, CPU-Verarbeitungszeit, die Gesamtanzahl der Client-Aufgaben, aktive Aufgaben, High-Watermark-Aufgaben, die maximal zulässigen Aufgaben, die Gesamtanzahl der Verbindungsversuche, die akzeptierten Verbindungen, die aktiven Verbindungen, die Anzahl der gesendeten und empfangenen Nachrichten sowie die Anzahl der gesendeten und empfangenen Datenbytes.</li> <li>- Zugriffsmethoden. Berichtet für jede Zugriffsmethode für jede aktive Aufgabe über die Anzahl der gelesenen und geschriebenen Zeilen, die Anzahl der gelesenen und geschriebenen Datenbytes, den Quell- oder Zieldateinamen oder den Daten-Mapping-Dateinamen je nach der Zugriffsmethode sowie über die CPU-Verarbeitungszeit.</li> <li>- Clients. Berichtet für jede aktive Aufgabe über die Aufgaben-ID, den Status, die Zugriffsmethode, den Lese- oder Schreibmodus, die Prozess- und Sitzungs-IDs (sofern verfügbar), die CPU-Verarbeitungszeit und Startdatum und -uhrzeit. Berichtet auch die Portnummer und IP-Adresse des Clients, der die Anfrage ausgegeben hat, für welche die Aufgabe erstellt wurde. Berichtet die PowerCenter-Sitzungs-ID und den Anwendungsnamen für CDC, wenn der Client PowerCenter ist.</li> </ul> <p>Der Standardwert lautet „Listener“.</p> <p><b>Hinweis:</b> In diesen Berichten kann eine Zugriffsmethode ein Quelltyp sein, z. B. NRDB. Eine Client-Aufgabe kann möglicherweise mehreren Zugriffsmethoden zugeordnet sein: einer Methode für das Lesen der Quelldaten und einer Methode für das Zuordnen von nicht-relationalen Daten zu einem relationalen Format.</p>

## DisplayStatusLogger

Zeigt den Status der Writer-Unteraufgabe für einen PowerExchange-Protokollierungsdienst an.

Mit dem Befehl `infacmd pwx DisplayStatusLogger` kann beispielsweise angegeben werden, wann der Writer die folgenden Aktionen abschließt:

- Initialisieren

- Lesen von oder Warten auf Quelldaten
- Schreiben von Quelldaten in eine Protokolldatei des Protokollierungsdiensts
- Schreiben von CDCT-Datensätzen während eines Dateiwechsels
- Löschen abgelaufener CDCT-Datensätze
- Herunterfahren

Der Befehl „infacmd pwx DisplayStatusLogger“ verwendet die folgende Syntax:

```
DisplayStatusLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx DisplayStatusLogger“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Protokollierungsdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.



Option	Argument	Beschreibung
-OSUser -oun	OS_user_name	<p>Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem.</p> <p>Aktivieren Sie Betriebssystemsicherheit wie folgt:</p> <ul style="list-style-type: none"> <li>- Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren.</li> <li>- Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.</li> </ul>
-OSPassword -oup	OS_password	<p>Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem.</p> <p>Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.</p>
-OSEPassword -ouep	OS_epassword	<p>Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem.</p> <p>Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.</p>

## FileSwitchLogger

Schließt geöffnete Protokolldateien für den PowerExchange-Protokollierungsdienst und wechselt dann zu einem neuen Satz an Protokolldateien. Wenn die geöffneten Logdateien keine Daten enthalten, findet kein Dateiwechsel statt.

**Hinweis:** Wenn Sie den fortlaufenden Extraktionsmodus verwenden, müssen Sie die Dateiwechsel in der Regel nicht manuell abschließen.

Der Befehl „infacmd pwx FileSwitchLogger“ verwendet die folgende Syntax:

```
FileSwitchLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx FileSwitchLogger“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Protokollierungsdiensts.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-OSUser -oun	OS_user_name	Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem.  Aktivieren Sie Betriebssystemsicherheit wie folgt: <ul style="list-style-type: none"> <li>- Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren.</li> <li>- Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.</li> </ul>

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	<p>Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem.</p> <p>Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.</p>
-OSEPassword -ouep	OS_epassword	<p>Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem.</p> <p>Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.</p>

## ListTaskListener

Zeigt Informationen zu jeder aktiven Aufgabe für den PowerExchange-Listenerdienst an, einschließlich TCP/IP-Adresse, Portnummer, Anwendungsname, Zugriffstyp und Status.

Der Befehl „`infacmd pwx ListTaskListener`“ verwendet die folgende Syntax:

```
ListTaskListener
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx ListTaskListener“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Listenerdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	<p>Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.</p>
-OSUser -oun	OS_user_name	<p>Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem.</p> <p>Aktivieren Sie Betriebssystemsicherheit wie folgt:</p> <ul style="list-style-type: none"> <li>- Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren.</li> <li>- Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.</li> </ul>

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	<p>Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem.</p> <p>Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.</p>
-OSEPassword -oue	OS_epassword	<p>Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem.</p> <p>Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.</p>

## ShutDownLogger

Hält den PowerExchange-Protokollierungsdienst in kontrollierter Weise an. Der Befehl schließt die Protokolldateien des Protokollierungsdiensts und schreibt die aktuelle Neustartposition dann in die CDCT-Datei.

Verwenden Sie diesen Befehl zum Anhalten eines PowerExchange-Protokollierungsdiensts, der im fortlaufenden Modus ausgeführt wird.

Beim Herunterfahren schließt der Protokollierungsdienst die folgenden Aktionen ab:

- Schließen aller geöffneten Logdateien
- Schreibt aktualisierte Informationen in die CDCT-Datei, einschließlich Neustart- und Sequenztoken
- Schließen der CAPI
- Anhalten der Writer- und Command Handler-Unteraufgaben
- Beenden des pwxcccl-Programms
- Aufzeichnen der CPU-Nutzung

Der Befehl „infacmd pwx ShutDownLogger“ verwendet die folgende Syntax:

```
ShutDownLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx ShutDownLogger“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Protokollierungsdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.



Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	<p>Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.</p>
-OSUser -oun	OS_user_name	<p>Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem.</p> <p>Aktivieren Sie Betriebssystemsicherheit wie folgt:</p> <ul style="list-style-type: none"> <li>- Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren.</li> <li>- Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.</li> </ul>

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	<p>Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem.</p> <p>Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.</p>
-OSEPassword -ouep	OS_epassword	<p>Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem.</p> <p>Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.</p>

## StopTaskListener

Hält eine PowerExchange-Listenerdienst-Aufgabe basierend auf einem Anwendungsnamen oder einer Aufgaben-ID an, die vom Benutzer angegeben wurde. Bei der Extraktion geänderter Daten wartet der Befehl „infacmd pwx StopTaskListener“ mit dem Anhalten der Aufgabe, bis entweder das UOW-Ende oder der Commit-Schwellenwert erreicht ist.

Der Befehl „infacmd pwx StopTaskListener“ verwendet die folgende Syntax:

```
StopTaskListener
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
[<-applicationid|-a> appname]
[<-taskid|-t> taskid]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx StopTaskListener“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Listenerdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	<p>Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.</p>
-OSUser -oun	OS_user_name	<p>Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem.</p> <p>Aktivieren Sie Betriebssystemsicherheit wie folgt:</p> <ul style="list-style-type: none"> <li>- Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren.</li> <li>- Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.</li> </ul>
-OSPassword -oup	OS_password	<p>Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem.</p> <p>Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.</p>

Option	Argument	Beschreibung
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem.  Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.
-applicationid -a	appname	Erforderlich, wenn Sie -taskid nicht angeben. Anwendungsname. Der Name des aktiven Extraktionsvorgangs, der angehalten werden soll. Die PWX-00712-Meldung der infacmd pwx listtaskListener-Befehlsausgabe zeigt diesen Namen an.
-taskid -t	taskid	Erforderlich, wenn Sie -application nicht angeben. Aufgaben-ID des Listenerdiensts. Die numerische ID für die Listenerdienstsaufgabe, die angehalten werden soll. <b>Tipp:</b> Um den Namen der aktiven Aufgabe zu bestimmen, verwenden Sie den Befehl infacmd pwx listtaskListener. In der Befehlsausgabe zeigt der Namenwert in der PWX-00712-Meldung die Aufgaben-ID an.

## UpgradeModels

Aktualisiert nichtrelationale Datenobjekte von PowerExchange 9.0.1. Sie müssen die Datenobjekte upgraden, bevor Sie sie verwenden können.

Der Befehl zeigt die Ergebnisse des Upgrades sortiert nach Verbindungsname, Schema und Map-Name an. Sie können den UpgradeModels-Befehl mehrmals ausführen, wenn bestimmte Objekte nicht beim ersten Mal aktualisiert werden.

Der Befehl überprüft, ob das Daten-Mapping mit den nichtrelationalen Operationen übereinstimmt, die dafür beim Importieren des nichtrelationalen Objekts definiert wurden. Wenn Abweichungen bestehen, werden die nichtrelationalen Operationen gelöscht und neu erstellt, um mit dem Daten-Mapping übereinzustimmen. Sie müssen alle betroffenen Mappings oder Mapplets ändern, um die neu erstellten nichtrelationalen Operationen zu verwenden.

Der Befehl „infacmd pwx UpgradeModels“ verwendet die folgende Syntax:

```
UpgradeModels
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-MrsServiceName|-msn> mrs_service_name
<-ConnectionName|-cn> connection_name
<-DataObjectSchemaName|-ds> data_object_schema_name
<-DataObjectName|-do> data_object_name
```

```

<-Preview|pr> preview

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-ServiceName|-sn> service_name]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx UpgradeModels“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-MrsServiceName -msn	mrs_service_name	Erforderlich. Name des Modellrepository-Dienst.  Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf nicht länger als 230 Zeichen sein und keine führenden oder abschließenden Leerzeichen, Wagenrückläufe, Tabulatoren oder die folgenden Zeichen enthalten:  / * ? < > "
-ConnectionName -cn	connection_name	Erforderlich. Name der Verbindung, die die nichtrelationalen Datenobjekte enthält, die aktualisiert werden sollen. Um alle Verbindungen oder alle Verbindungen mit dem gleichen Anfangsnamensmuster anzugeben, setzen Sie das Platzhalterzeichen Sternchen (*) in doppelte Anführungszeichen, z. B. "*" oder ABC"*".
-DataObjectSchemaName -ds	data_object_schema_name	Erforderlich. Name des Schemas, das die Datenzuordnungen der nichtrelationalen Datenobjekte enthält, die aktualisiert werden sollen. Um alle Schemas oder alle Schemas mit dem gleichen Anfangsnamensmuster anzugeben, setzen Sie das Platzhalterzeichen Sternchen (*) in doppelte Anführungszeichen, z. B. "*" oder ABC"*".

Option	Argument	Beschreibung
-DataObjectName -do	data_object_name	Erforderlich. Name der Datenzuordnung des nichtrelationalen Datenobjekts, das aktualisiert werden soll. Um alle Datenzuordnungen oder alle Datenzuordnungen mit dem gleichen Anfangsnamensmuster anzugeben, setzen Sie das Platzhalterzeichen Sternchen (*) in doppelte Anführungszeichen, z. B. "*" oder ABC"*".
-Preview -pr	Vorschau	Erforderlich. Geben Sie „Y“ an, um eine Vorschau der Upgrade-Ergebnisse anzuzeigen, ohne diese zu bestätigen. Geben Sie „N“ an, um ein Upgrade der Objekte durchzuführen. Um eine erfolgreiche Ausführung des Befehls sicherzustellen, legen Sie „Preview“ auf „Y“ fest und führen den UpgradeModels-Befehl aus, bevor Sie das tatsächliche Upgrade durchführen.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Optional. Name des Listenerdiensts.  Der Befehl verwendet zuerst den Verbindungsnamen zum Abrufen der angegebenen Daten-Mappings. Wenn der Versuch fehlschlägt, verwendet der Befehl den Namen des Listenerdiensts zum Abrufen von Daten-Mappings.  Bei diesem Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Der Name darf nicht länger als 128 Zeichen sein und keine Wagenrückläufe, Tabulatoren, Leerzeichen oder die folgenden Zeichen enthalten:  / * ? < > "

# UpdateListenerService

Aktualisiert die Eigenschaften eines PowerExchange-Listenerdiensts.

Der Befehl „infacmd pwx UpdateListenerService“ verwendet die folgende Syntax:

```
UpdateListenerService

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

[<-LicenseName|-ln> license_name]

[<-NodeName|-nn> node_name]

[<-BackupNode|-bn> backup_node]

[<-StartParameters|-sp> start_parameters>]

[<-SvcPort|-sp> service_port]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx UpdateListenerService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.



Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/ Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Listenerdiensts.

Option	Argument	Beschreibung
-LicenseName -ln	license_name	Optional. Lizenz zur Zuweisung zum Dienst. Wenn nicht bereits bereitgestellt, erforderlich, bevor Sie den Dienst aktivieren können.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Listenerdienst ausgeführt werden soll.
-BackupNode -bn	backup_node	Optional. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, wird mit dieser Option der Name des Backup-Knotens angegeben.

Option	Argument	Beschreibung
-StartParameters -sp	start_parameters	<p>Optional. Parameter, die beim Starten des Listenerdiensts einbezogen werden müssen. Trennen Sie die Parameter durch Leerzeichen.</p> <p>Sie können die folgenden Parameter einbeziehen:</p> <ul style="list-style-type: none"> <li>- <i>node_name</i> Knotenname, der den Listenerdienst identifiziert. Dieser Name muss mit dem Namen in der LISTENER-Anweisung in der Konfigurationsdatei DBMOVER übereinstimmen.</li> <li>- <i>config=directory</i> Gibt den vollständigen Pfad und Dateinamen für die Konfigurationsdatei „dbmover.cfg“ an, die Sie anstelle der Standarddatei „dbmover.cfg“ verwenden möchten. Diese alternative Konfigurationsdatei hat Vorrang vor jeder anderen alternativen Konfigurationsdatei, die Sie in der Umgebungsvariable PWX_CONFIG angeben.</li> <li>- <i>license=directory/license_key_file</i> Gibt den vollständigen Pfad und Dateinamen für eine Lizenzschlüsseldatei an, die Sie anstelle der Standarddatei license.key verwenden möchten. Diese alternative Lizenzschlüsseldatei und die Standarddatei dürfen nicht denselben Namen und denselben Pfad haben. Entweder Name oder Pfad muss unterschiedlich sein. Diese alternative Lizenzschlüsseldatei hat Vorrang vor jeder anderen alternativen Lizenzschlüsseldatei, die Sie in der Umgebungsvariable PWX_LICENSE angeben.</li> </ul> <p><b>Hinweis:</b> In den Konfigurations- und Lizenzparametern müssen Sie den vollständigen Pfad nur dann angeben, wenn die Datei sich <i>nicht</i> im Installationsverzeichnis befindet. Schließen Sie Pfad- und Dateinamen, die Leerzeichen enthalten, in Anführungszeichen ein.</p>
-SvcPort -sp	service_port	<p>Optional. Port des Listenerdiensts für die Reaktion auf Befehle vom Dienstmanager.</p>

# UpdateLoggerService

Aktualisiert die Eigenschaften eines PowerExchange-Protokollierungsdiensts.

Der Befehl „infacmd pwx UpdateLoggerService“ verwendet die folgende Syntax:

```
UpdateLoggerService

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

[<-LicenseName|-ln> license_name]

[<-BackupNode|-bn> backup_node]

[<-StartParameters|-sp> start_parameters>]

[<-SvcPort|-sp> service_port]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx UpdateLoggerService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie den Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Protokollierungsdiensts.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Protokollierungsdienst ausgeführt werden soll.
-LicenseName -ln	license_name	Lizenz zur Zuweisung zum Dienst. Wenn nicht bereits bereitgestellt, erforderlich, bevor Sie den Dienst aktivieren können.
-BackupNode -bn	backup_node	Optional. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, wird mit dieser Option der Name des Backup-Knotens angegeben.

Option	Argument	Beschreibung
-StartParameters -sp	start_parameters	<p>Optional. Parameter, die beim Starten des Protokollierungsdiensts einbezogen werden müssen. Trennen Sie die Parameter durch Leerzeichen.</p> <p>Sie können die folgenden Parameter einbeziehen:</p> <ul style="list-style-type: none"> <li>- coldstart={Y N} Gibt an, ob der Protokollierungsdienst kalt oder warm gestartet wird. Geben Sie Y für einen Kaltstart des Protokollierungsdiensts ein. Wenn die CDCT-Datei Protokolldatensätze enthält, löscht der Protokollierungsdienst diese Datensätze. Geben Sie N ein, um den Protokollierungsdienst ab dem Neustartpunkt warm zu starten, der in der CDCT-Datei angegeben ist. Standardwert ist „N“.</li> <li>- config=directory/pwx_config_file Gibt den vollständigen Pfad und Dateinamen für die Konfigurationsdatei „dbmover.cfg“ an, die Sie anstelle der Standarddatei „dbmover.cfg“ verwenden möchten. Diese alternative Konfigurationsdatei hat Vorrang vor jeder anderen alternativen Konfigurationsdatei, die Sie in der Umgebungsvariable PWX_CONFIG angeben.</li> <li>- cs=directory/pwxlogger_config_file Gibt den Pfad und Dateinamen für die Konfigurationsdatei des Protokollierungsdiensts an. Sie können auch den cs-Parameter verwenden, um eine Protokollierungsdienst-Konfigurationsdatei anzugeben, die die Standarddatei pwxcl.cfg überschreibt. Diese Überschreibungsdatei und die Standarddatei dürfen nicht denselben Namen und denselben Pfad haben. Entweder Name oder Pfad muss unterschiedlich sein.</li> <li>- encryptepwd=encrypted_password Ein Passwort im verschlüsselten Format zum Aktivieren der Verschlüsselung von Protokolldateien der PowerExchange-Protokollierung. Mit diesem Passwort kann die PowerExchange-Protokollierung einen eindeutigen Verschlüsselungsschlüssel für jede Protokolldatei der Protokollierung erzeugen. Das Passwort wird in der CDCT-Datei im verschlüsselten Format gespeichert. Aus Sicherheitsgründen wird das Passwort weder in CDCT-Sicherungsdateien gespeichert noch in den CDCT-Berichten angezeigt, die mit dem PowerExchange-Dienstprogramm PWXUCDCT erzeugt werden können. Bei Angabe dieses Parameters müssen Sie auch coldstart=y angeben. Wenn Sie diesen Parameter und den Parameter ENCRYPTEPWD in der Konfigurationsdatei (pwxcl.cfg) der PowerExchange-Protokollierung angeben, hat der Parameter in der Konfigurationsdatei Vorrang. Wenn Sie diesen Parameter und den Parameter ENCRYPTPWD in der Konfigurationsdatei der PowerExchange-Protokollierung angeben, tritt ein Fehler auf. Sie können den AES-Algorithmus festlegen, um ihn zum Verschlüsseln der Protokolldatei im Parameter ENCRYPTOPT der Datei „pwxcl.cfg“ zu verwenden. Standardwert ist AES128.</li> </ul>

Option	Argument	Beschreibung
		<p><b>Tipp:</b> Zur Sicherheitsoptimierung empfiehlt Informatica, das Verschlüsselungspasswort beim Kaltstart der PowerExchange-Protokollierung und nicht in der Konfigurationsdatei „pwxcl.cfg“ anzugeben. Mit dieser Vorgehensweise verringern Sie aus folgenden Gründen das Risiko eines böswilligen Zugriffs auf das Verschlüsselungspasswort: 1) Das Verschlüsselungspasswort ist nicht in der Datei „pwxcl.cfg“ gespeichert. 2) Sie können das Passwort nach einem erfolgreichen Kaltstart aus der Befehlszeile löschen. Wenn Sie das Verschlüsselungspasswort für einen Kaltstart angeben und die CDCT-Datei dann zu einem späteren Zeitpunkt wiederherstellen müssen, müssen Sie dasselbe Verschlüsselungspasswort im Befehl RESTORE_CDCT des Dienstprogramms PWXUCDCT eingeben.</p> <p>Um die Protokolldateien der PowerExchange-Protokollierung <i>nicht</i> zu verschlüsseln, geben Sie kein Verschlüsselungspasswort ein.</p> <ul style="list-style-type: none"> <li>- license=directory/license_key_file Gibt den vollständigen Pfad und Dateinamen für eine Lizenzschlüsseldatei an, die Sie anstelle der Standarddatei license.key verwenden möchten. Diese alternative Lizenzschlüsseldatei und die Standarddatei dürfen nicht denselben Namen und denselben Pfad haben. Entweder Name oder Pfad muss unterschiedlich sein. Diese alternative Lizenzschlüsseldatei hat Vorrang vor jeder anderen alternativen Lizenzschlüsseldatei, die Sie in der Umgebungsvariable PWX_LICENSE angeben.</li> <li>- specialstart={Y N} Gibt an, ob ein Sonderstart der PowerExchange-Protokollierung durchgeführt werden soll. Ein Sonderstart startet die Verarbeitung der PowerExchange-Erfassung an dem Punkt im Änderungsstrom, den Sie in der Datei „pwxcl.cfg“ angeben. Dieser Startpunkt überschreibt den Neustartpunkt aus der CDCT-Datei für die PowerExchange-Protokollierungsausführung. Bei einem Sonderstart wird kein Inhalt aus der CDCT-Datei gelöscht.</li> </ul> <p>Verwenden Sie diesen Parameter zum Überspringen problematischer Stellen in den Quellprotokollen, ohne dabei erfasste Daten zu verlieren. Verwenden Sie einen Sonderstart beispielsweise in folgenden Situationen:</p> <ul style="list-style-type: none"> <li>- Sie möchten nicht, dass die PowerExchange-Protokollierung eine Aktualisierung eines Oracle-Katalogs erfasst. Stoppen Sie in diesem Fall die PowerExchange-Protokollierung vor der Aktualisierung. Erzeugen Sie nach Abschluss der Aktualisierung eine neue Sequenz und starten Sie Token für die PowerExchange-Protokollierung basierend auf dem Post-Upgrade-SCN neu. Geben Sie diese Token-Werte in den Parametern SEQUENCE_TOKEN und RESTART_TOKEN in der Datei „pwxcl.cfg“ ein und führen Sie dann einen Sonderstart der PowerExchange-Protokollierung durch.</li> <li>- Sie möchten nicht, dass von der PowerExchange-Protokollierung alte, nicht verfügbare Protokolle erneut verarbeitet werden, die durch ausstehende Arbeitseinheiten verursacht wurden, die nicht zu CDC gehören. Stoppen Sie in diesem Fall die PowerExchange-</li> </ul>

Option	Argument	Beschreibung
		<p>Protokollierung. Bearbeiten Sie den Wert RESTART_TOKEN, um den SCN des frühesten verfügbaren Protokolls widerzuspiegeln, und führen Sie dann einen Sonderstart durch. Wenn alle ausstehenden Arbeitseinheiten, die vor diesem Neustartpunkt gestartet wurden, zu CDC gehören, gehen unter Umständen Daten verloren.</p> <p>Gültige Werte:</p> <ul style="list-style-type: none"> <li>- Y. Führen Sie einen Sonderstart der PowerExchange-Protokollierung ab dem Punkt im Änderungsstrom durch, der von den Parameterwerten SEQUENCE_TOKEN und RESTART_TOKEN in der Konfigurationsdatei „pwxcl.cfg“ definiert wird. Sie müssen gültige Token-Werte in der Datei „pwxcl.cfg“ angeben, um einen Sonderstart durchzuführen. Diese Token-Werte überschreiben die Token-Werte aus der CDCT-Datei. Stellen Sie sicher, dass der Wert SEQUENCE_TOKEN in der Datei „pwxcl.cfg“ größer oder gleich dem aktuellen Sequenz-Token in der CDCT-Datei ist.</li> </ul> <p>Geben Sie den Parameter coldstart=Y nicht noch zusätzlich an. Wenn Sie den Parameter coldstart=Y angeben, hat dieser Parameter Vorrang.</p> <ul style="list-style-type: none"> <li>- N. Führen Sie keinen Sonderstart durch. Führen Sie einen Kalt- oder Warmstart, wie vom coldstart-Parameter angegeben, durch.</li> </ul> <p>Standardwert ist „N“.</p> <p><b>Hinweis:</b> In den Konfigurations-, cs- und Lizenzparametern müssen Sie den vollständigen Pfad nur dann angeben, wenn die Datei sich <i>nicht</i> im Installationsverzeichnis befindet. Schließen Sie Pfad- und Dateinamen, die Leerzeichen enthalten, in Anführungszeichen ein.</p>
-SvcPort -sp	service_port	Port des Protokollierungsdiensts für die Reaktion auf Befehle vom Dienstmanager.



# KAPITEL 30

## infacmd roh-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [listProcessProperties, 1101](#)
- [listReverseProxyServerOptions, 1103](#)
- [listServiceProcessOptions, 1104](#)
- [listServiceOptions, 1106](#)
- [updateReverseProxyServerOptions, 1107](#)
- [updateServiceProcessOptions, 1110](#)
- [updateServiceOptions, 1111](#)

### listProcessProperties

Listet die REST Operations Hub-Prozesseigenschaften auf.

Der Befehl „infacmd roh listProcessProperties“ verwendet folgende Syntax:

```
<-DomainName|-dn> domain_name  
<-UserName|-un> user_name  
<-Password|-pd> password  
[<-SecurityDomain|-sdn> security_domain]  
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd roh listProcessProperties“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domännennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domännennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user-name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomännennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	Host des Domänen-Gateways:Port	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Geben Sie den Hostnamen und die Portnummer für den Gateway-Knoten in der Domäne ein.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariablen INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

# listReverseProxyServerOptions

Listet die Reverse-Proxy-Server-Eigenschaften auf.

Der Befehl „infacmd roh listReverseProxyServerOptions“ verwendet folgende Syntax:

```
<-DomainName|-dn> domain_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-SecurityDomain|-sdn> security_domain]  
  
[<-NodeName|-nn> Node_name]  
  
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd roh listReverseProxyServerOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Beim Namen der Sicherheitsdomäne wird zwischen Groß- und Kleinschreibung unterschieden. Wenn für die Domäne die native oder LDAP-Authentifizierung verwendet wird, ist „Nativ“ der Standardwert. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-NodeName -nn	Knotenname	Erforderlich. Knoten, auf dem der Dienstprozess ausgeführt wird.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariablen INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## listServiceProcessOptions

Listet die Prozesseigenschaften des REST Operations Hub-Dienstes auf.

Der Befehl „infacmd roh listServiceProcessOptions“ verwendet folgende Syntax:

```
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-NodeName|-nn> Node_name]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd roh listServiceProcessOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Beim Namen der Sicherheitsdomäne wird zwischen Groß- und Kleinschreibung unterschieden. Wenn für die Domäne die native oder LDAP-Authentifizierung verwendet wird, ist „Nativ“ der Standardwert. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-NodeName -nn	Knotenname	Erforderlich. Knoten, auf dem der Dienstprozess ausgeführt wird.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariablen INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## listServiceOptions

Listet die Eigenschaften des REST Operations Hub-Diensts auf.

Der Befehl „infacmd roh listServiceOptions“ verwendet die folgende Syntax:

```
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd roh listServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Beim Namen der Sicherheitsdomäne wird zwischen Groß- und Kleinschreibung unterschieden. Wenn für die Domäne die native oder LDAP-Authentifizierung verwendet wird, ist „Nativ“ der Standardwert. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## updateReverseProxyServerOptions

Aktualisiert die Reverse-Proxy-Server-Eigenschaften.

Der Befehl „infacmd roh updateReverseProxyServerOptions“ verwendet folgende Syntax:

```
<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-NodeName|-nn> Node_name

[<-ServiceProcessReverseProxyServerOptions|-so> option_name=value ...
(EnableReverseProxyServer, URLScheme, httpPortForRPS, httpsPortForRPS,
ReverseProxyServerSSLCertificate,
```

```
ReverseProxyServerSSLCertificateKey, ReverseProxyServerSSLCertificatePassPhrasePath,
VerifyIncomingClients,
SSLClientCertificatePathForIncomingClients, SSLCertificatePathForUpstreamServer,
SSLCertificateKeyForUpstreamServer, SSLCertificatePassPhrasePathForUpstreamServer)
```

Information regarding ReverseProxyServer https mode...(ReverseProxyServerSSLCertificate, ReverseProxyServerSSLCertificateKey, SSLClientCertificatePathForIncomingClients, VerifyIncomingClients are applicable when https mode is enabled)]

```
[<-Options|-o options]
```

```
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd roh updateReverseProxyServerOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.



Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Beim Namen der Sicherheitsdomäne wird zwischen Groß- und Kleinschreibung unterschieden. Wenn für die Domäne die native oder LDAP-Authentifizierung verwendet wird, ist „Nativ“ der Standardwert. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-NodeName -nn	Knotenname	Erforderlich. Knoten, auf dem der Dienstprozess ausgeführt wird.
- ServiceProcessReverseProxyServerOptions -so	option_name=value ...	Optional. Dienstprozesseigenschaften, die definieren, wie der Reverse-Proxy-Server ausgeführt wird.
-Options -o	Option	Optional. Geben Sie jede benutzerdefinierte Eigenschaftsoption durch ein Leerzeichen getrennt ein. Verwenden Sie das Präfix RPS: mit dem Name-Wert-Paar. Beispiel: RPS:<custom_property>=<custom_value>.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

# updateServiceProcessOptions

Aktualisiert die Eigenschaften von Rest Operations Hub-Dienstprozessen in einer Domäne.

Der Befehl „infacmd roh updateServiceProcessOptions“ verwendet folgende Syntax:

```
<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-NodeName|-nn> Node_name

[<-ServiceOptions|-so> option_name=value ...(httpPort, httpsPort, keystoreFile,
keystorePass, SSLProtocol)]

[<-Options|-o options]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd roh updateServiceProcessOption“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Beim Namen der Sicherheitsdomäne wird zwischen Groß- und Kleinschreibung unterschieden. Wenn für die Domäne die native oder LDAP-Authentifizierung verwendet wird, ist „Nativ“ der Standardwert. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-NodeName -nn	Knotenname	Erforderlich. Knoten, auf dem der Dienstprozess ausgeführt wird.
-ServiceOptions -so	option_name=value ...	Optional. Diensteigenschaften, die definieren, wie der REST Operations Hub-Dienst ausgeführt wird.
-Options -o	Option	Optional. Geben Sie jede benutzerdefinierte Eigenschaftsoption durch ein Leerzeichen getrennt ein. Verwenden Sie das Präfix ROH: mit dem Name-Wert-Paar. Beispiel: ROH:<custom_property>=<custom_value>.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## updateServiceOptions

Aktualisiert die Diensteigenschaften für den REST Operations Hub.

Der Befehl „infacmd roh updateServiceOptions“ verwendet die folgende Syntax:

```
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
```

```
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-NodeName|-nn> node_name|<-GridName|-gn> grid_name]

[<-Options|-o options]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd roh updateServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Beim Namen der Sicherheitsdomäne wird zwischen Groß- und Kleinschreibung unterschieden. Wenn für die Domäne die native oder LDAP-Authentifizierung verwendet wird, ist „Nativ“ der Standardwert. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-NodeName -nn	Knotenname	Erforderlich. Knotenname, der zu einem Gitter gehört, wo der Dienstprozess ausgeführt wird.
-GridName -gn	grid_name	Erforderlich. Name des Gitters.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Options -o	Option	Optional. Geben Sie jede benutzerdefinierte Eigenschaftsoption durch ein Leerzeichen getrennt ein. Verwenden Sie das Präfix <code>RPS:</code> , um die benutzerdefinierte Eigenschaft des Reverse-Proxy-Servers, oder <code>ROH:</code> , um die benutzerdefinierte Eigenschaft des REST Operations Hub festzulegen. Beispiel: <code>RPS:&lt;custom_property&gt;=&lt;custom_value&gt;.</code>

# KAPITEL 31

## infacmd rms-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [ListComputeNodeAttributes, 1114](#)
- [ListServiceOptions, 1116](#)
- [SetComputeNodeAttributes, 1117](#)
- [UpdateServiceOptions, 1119](#)

### ListComputeNodeAttributes

Listet die Attribute des Berechnungsknotens auf, die für den angegebenen oder für alle Knoten übersprungen wurden. Verwenden Sie den infacmd rms SetComputeNodeAttributes-Befehl, um die Attribute des Berechnungsknotens zu überspringen.

Bei den Standardwerten für die Attribute handelt es sich um die tatsächliche Anzahl der Kerne und den auf dem Computer verfügbaren Speicher. Wenn der infacmd rms ListComputeNodeAttributes-Befehl keinen Wert für ein Attribut auflistet, verwendet der Ressourcenmanager-Dienst die Standardwerte.

Der infacmd rms ListComputeNodeAttributes-Befehl verwendet die folgende Syntax:

```
ListComputeNodeAttributes  
  
<-DomainName|-dn> domain_name  
  
[<-SecurityDomain|-sdn> security_domain]  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-NodeName|-nn> node_name]  
  
[<-ServiceName|-sn> service_name]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd rms ListComputeNodeAttributes“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-NodeName -nn	node_name	Optional. Name des Berechnungsknotens, für den die Attribute aufgelistet werden sollen.  Wenn Sie die Option nicht angeben, listet der Befehl den Attributsatz für alle Berechnungsknoten in der Domäne auf.
-ServiceName -sn	service_name	Optional. Geben Sie Resource_Manager_Service ein.

# ListServiceOptions

Listet die Eigenschaften für den Ressourcenmanager-Dienst auf.

Der `infacmd rms ListServiceOptions`-Befehl verwendet die folgende Syntax:

```
ListServiceOptions  
  
<-DomainName|-dn> domain_name  
  
[<-SecurityDomain|-sdn> security_domain]  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-ServiceName|-sn> service_name]  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd rms ListServiceOptions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>



Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Optional. Geben Sie Resource_Manager_Service ein.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## SetComputeNodeAttributes

Überschreibt die Berechnungsknotenattribute für den angegebenen Knoten.

Bei den Standardwerten für die Attribute handelt es sich um die tatsächliche Anzahl der Kerne und den auf dem Computer verfügbaren Speicher. Zum Zurücksetzen einer Option auf ihren Standardwert geben Sie -1 als Wert ein.

Der infacmd rms SetComputeNodeAttributes-Befehl verwendet die folgende Syntax:

```
SetComputeNodeAttributes
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-NodeName|-nn> node_name
```

```
[<-MaxCores|-mc> max_number_of_cores_to_allocate]
```

```
[<-MaxMem|-mm> max_memory_in_mb_to_allocate]
```

```
[<-ServiceName|-sn> service_name]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd rms SetComputeNodeAttributes“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-NodeName -nn	node_name	Erforderlich. Name des Berechnungsknotens, für den Attribute festgelegt werden sollen.

Option	Argument	Beschreibung
-MaxCores -mc	max_number_of_cores_to_allocate	Optional. Maximale Anzahl der Kerne, die der Ressourcenmanager-Dienst für Jobs zuweisen kann, die auf dem Berechnungsknoten ausgeführt werden. Ein Berechnungsknoten benötigt mindestens fünf verfügbare Knoten, um einen Container zum Starten eines DTM-Prozesses zu initialisieren. Wenn ein beliebiger dem Gitter zugewiesener Berechnungsknoten weniger als fünf Kerne aufweist, wird diese Anzahl als Mindestanzahl der Kerne verwendet, die zum Initialisieren eines Containers notwendig sind.  Standardmäßig stellt die maximale Anzahl der Kerne die tatsächliche Anzahl der auf dem Computer verfügbaren Kerne dar.
-MaxMem -mm	max_memory_in_mb_to_allocate	Optional. Maximale Speichermenge in Megabyte, die vom Ressourcenmanager-Dienst für Jobs zugewiesen werden kann, die auf dem Berechnungsknoten ausgeführt werden. Ein Berechnungsknoten benötigt mindestens 2,5 GB Speicher, um einen Container zum Starten eines DTM-Prozesses zu initialisieren.  Standardmäßig stellt die maximale Speichermenge die tatsächlich auf dem Computer verfügbare Speichermenge dar.
-ServiceName -sn	service_name	Optional. Geben Sie Resource_Manager_Service ein.

## UpdateServiceOptions

Aktualisiert die Eigenschaften des Ressourcenmanager-Diensts. Führen Sie diesen Befehl aus, um den primären und den Backup-Knoten für den Ressourcenmanager-Dienst zu konfigurieren.

Sie können die Eigenschaften ändern, während der Dienst ausgeführt wird, aber Sie müssen den Dienst neu starten, damit die geänderten Eigenschaften wirksam werden.

Der Befehl „`infacmd rms UpdateServiceOptions`“ verwendet die folgende Syntax:

```
UpdateServiceOptions
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
[<-ServiceName|-sn> service_name]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-Options|-o> options]
[<-NodeName|-nn> primary_node_name]
[<-BackupNodes|-bn> backup_node_name1,backup_node_name2,...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd rms UpdateServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Optional. Geben Sie Resource_Manager_Service ein.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Options -o	options	Optional. Geben Sie jede Option durch ein Leerzeichen getrennt ein.
-NodeName -nn	primary_node_name	Optional. Primärer Knoten, auf dem der Ressourcenmanager-Dienst ausgeführt wird.
-BackupNodes -bn	backup_node_name1,backup_node_name2,...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist.

## Optionen des Ressourcenmanager-Diensts

Verwenden Sie die Optionen des Ressourcenmanager-Diensts mit dem infacmd rms UpdateServiceOptions-Befehl.

Geben Sie die Optionen des Ressourcenmanager-Diensts in folgendem Format ein:

```
... -o option_type.option_name=value
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Optionen des Ressourcenmanager-Diensts beschrieben:

Option	Beschreibung
ResourceManagerServiceOptions.Log_Level	Ebene der Fehlermeldungen, die der Ressourcenmanager-Dienst in das Dienstprotokoll schreibt. Wählen Sie eine der folgenden Meldungsebenen aus: Fatal, Error, Warning, Info, Trace oder Debug.

## KAPITEL 32

# infacmd rtm-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [DeployImport, 1122](#)
- [Export, 1124](#)
- [Import, 1127](#)

## DeployImport

Importiert den Inhalt aus einer Anwendungsdatei in der Datenbank, die vom Modellrepository gelesen wird.

Der Befehl „infacmd rtm DeployImport“ verwendet die folgende Syntax:

```
DeployImport
<-DomainName|-dn> Domain name
<-UserName|-un> User name
<-Password|-pd> Password
<-securityDomain|-sdn> Security domain
[<-Gateway|-hp> Domain gateway host:port]
[<-NodeName|-nn> Node name]
<-DataIntegrationService|-ds> Data Integration Service name
<-CodePage|-cp> Code page
<-Folder|-f> The folder to import from
<-MetadataFile|-mf> Metadata file
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd rtm DeployImport“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	Domänenname	Erforderlich. Name der Informatica-Domäne. Sie können den Domännennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domännennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-securityDomain -sdn	Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomännennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	Host des Domänen-Gateways:Port	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Geben Sie den Hostnamen und die Portnummer für den Gateway-Knoten in der Domäne ein. Verwenden Sie folgende Syntax: <code>gateway_hostname:HttpPort</code>
-NodeName -nn	Knotenname	Optional. Name des Gateway-Knotens für den Modellrepository-Dienst.

Option	Argument	Beschreibung
-DataIntegrationService -ds	Name des Datenintegrationssdiensts	Erforderlich. Name des Datenintegrationsdiensts.
-CodePage -cp	Codepage	Erforderlich. Codepage für die zu importierenden Referenzdaten.
-Folder -f	Der Ordner, aus dem importiert wird	Erforderlich. Pfad des Ordners, der die zu importierenden Dateien enthält. Sie führen den Befehl DeployImport auf dem Computer aus, auf dem der Ordner gespeichert ist. Die Ordneroption beschreibt einen Pfad auf dem Computer, auf dem der Befehl ausgeführt wird.
-MetadataFile -mf	Metadatendatei	Erforderlich. Vollständiger Name und Pfad für die Anwendungsdatei, auf die der Befehl angewendet wird.

## Export

Exportieren von Daten aus Referenztabellen. Sie können Referenztabellenobjekte oder nur die Daten exportieren. Sie können Daten aus verwalteten und nicht verwalteten Referenztabellen exportieren.

Definieren Sie die Exportdaten mit einer der folgenden Optionen:

- ProjectFolder. Name des Projekts oder Ordners, der exportiert werden soll.
- MetadataFile. Name einer metadata.xml-Datei, die auf die zu exportierenden Referenztabellen verweist.
- ObjectList. Vollständiger Pfad zu einer Textdatei, die eine Liste der zu exportierenden Dateien enthält.

Wenn Sie eine Objektliste konfigurieren, erstellen Sie eine Textdatei, die eine Liste von Objekten mit der folgenden Syntax enthält:

```
ProjectName/FolderName/reference_table_object1
ProjectName/FolderName/reference_table_object2
ProjectName/FolderName/reference_table_object3
```

**Hinweis:** Sie müssen jeden Pfad in der Objektliste mit Schrägstrichen konfigurieren. Verwenden Sie keine umgekehrten Schrägstriche im Pfad.

Der Befehl „`infacmd rtm Export`“ verwendet die folgende Syntax:

```
Export
<-DomainName|-dn> Domain name
<-UserName|-un> User name
<-Password|-pd> Password
<-SecurityDomain|-sdn> Security domain
[<-Gateway|-hp> Domain gateway host:port]
[<-NodeName|-nn> Node name]
<-RepositoryService|-rs> Model Repository Service name
```



<-CodePage|-cp> Code Page  
 <-Folder|-f> The folder to export to  
 [<-ObjectList|-ol> List of Objects to export]  
 [<-ProjectFolder|-pf> Name of the project folder to export]  
 [<-metadataFile|-mf> Metadata file]  
 [<-Recursive|-r> Include subfolders when exporting project folder]  
 [<-SkipDatGeneration|-sdg> Skip Data Generation]

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd rtm Export“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	Domänenname	<p>Erforderlich. Name der Informatica-Domäne.</p> <p>Sie können den Domännennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domännennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.</p>
-UserName -un	Benutzername	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	Passwort	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>

Option	Argument	Beschreibung
-SecurityDomain -sdn	Sicherheitsdomäne	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-Gateway -hp	Hostname des Domänen-Gateways:Portnummer	<p>Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Geben Sie den Hostnamen und die Portnummer für den Gateway-Knoten in der Domäne ein. Verwenden Sie folgende Syntax:</p> <pre>gateway_hostname:HttpPort</pre>
-NodeName -nn	Knotenname	Optional. Name des Gateway-Knotens für den Modellrepository-Dienst.
-RepositoryService -rs	Name des Modellrepository-Diensts	Name des Modellrepository-Diensts.
-CodePage -cp	Codepage	Erforderlich. Codepage für die Referenzdaten.
-Folder -f	Der Ordner, in den exportiert wird	Erforderlich. Zielspeicherort für die Exportdatei.
-ObjectList -ol	Liste der zu exportierenden Objekte	Vollständig qualifizierter Dateiname, der eine Liste der Referenztabelleobjekte enthält. Konfigurieren Sie diese Option nicht mit der Option ProjectFolder oder metadataFile.
-ProjectFolder -pf	Name des zu exportierenden Projektordners	<p>Name des Projekts und Ordners, die exportiert werden sollen. Verwenden Sie folgende Syntax:</p> <pre>ProjectName/FolderName</pre> <p>Verwenden Sie zur Konfiguration weder die Option metadataFile noch die Option ObjectList.</p>
-metadataFile -mf	Metadatendatei	<p>Erforderlich für den Export von Objekten. Vollständiger Pfad und Name für eine metadata.xml-Datei, auf die der Befehl angewendet werden soll. Exportiert alle Referenztabelle, die in der Datei „metadata.xml“ enthalten sind.</p> <p>Konfigurieren Sie diese Option nicht mit der Option ProjectFolder oder ObjectList.</p>

Option	Argument	Beschreibung
-Recursive -r	Beim Exportieren des Projektordners Unterordner berücksichtigen	Optional. Verwenden Sie diese Option mit der Option ProjectFolder. Exportieren Sie mehr als eine Ebene des Objekts. Standardwert ist „nicht rekursiv“.
-SkipDatGeneration -sdg	Datenerzeugung überspringen	Optional. Schreibt eine DAT-Datei, die die Struktur der Referenztable beschreibt, in den Verzeichnissatz in der Ordneigenschaft. Beim Importieren der Referenztable wird diese Datei nicht verwendet. Standardwert ist „False“.

## Import

Führt einen Metadaten- und Datenimport aus Objektexportdateien durch. Importiert Referenztabellen-Metadaten in das Modellrepository und importiert die Daten in die Referenzdaten-Datenbank. Importiert auch Referenzdaten ohne die Metadaten.

Bevor Sie Referenztabellendaten importieren, muss das Zielprojekt im Modellrepository vorhanden sein.

Der Befehl „`infacmd rtm Import`“ verwendet die folgende Syntax:

```

Import
<-DomainName|-dn> Domain name

<-UserName|-un> User name

<-Password|-pd> Password

<-securityDomain|-sdn> Security domain

[<-Gateway|-hp> Domain gateway host:port]

[<-NodeName|-nn> Node name]

<-RepositoryService|-rs> Model Repository Service name

<-CodePage|-cp> Code page

<-ConflictResolution|-cr> Conflict resolution

<-ImportType|-it> Import type

<-Folder|-f> The folder to import from

[<-FileName|-fn> Required only for importing a single dictionary]

[<-MetadataFile|-mf> Required only for Object import]

[<-ProjectFolder|-pf> Name of the project folder to import into]

[<-NotRecursive|-nr> Don't include subfolders]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd rtm Import“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	Domänenname	Erforderlich. Name der Informatica-Domäne. Sie können den Domännennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domännennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_USER</code> festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-securityDomain -sdn	Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomännennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	Host des Domänen-Gateways:Port	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Name und Portnummer für den Gateway-Knoten in der Domäne. Verwenden Sie folgende Syntax: <code>gateway_hostname:HttpPort</code>
-NodeName -nn	Knotenname	Optional. Name des Gateway-Knotens für den Modellrepository-Dienst.

Option	Argument	Beschreibung
-RepositoryService -rs	Name des Modellrepository-Diensts	Erforderlich. Name des Modellrepository-Diensts.
-CodePage -cp	Codepage	Erforderlich. Codepage für die Referenzdaten.
-ConflictResolution -cr	Konfliktlösung	<p>Erforderlich. Definiert das Verhalten bei Auftreten eines Namenskonflikts.</p> <p>Geben Sie eines der folgenden Argumente ein:</p> <ul style="list-style-type: none"> <li>- Replace. Ersetzen Sie das aktuelle Referenztabellenobjekt durch das Objekt, das Sie importieren.</li> <li>- Rename. Erstellen Sie ein Referenztabellenobjekt mit einem anderen Namen.</li> <li>- Skip. Importieren Sie die Referenztable nicht.</li> </ul> <p><b>Hinweis:</b> Das Replace-Argument gibt die Auflösungsrichtlinie für das Referenztabellenobjekt und nicht für die zugrunde liegende Tabelle in der Referenzdaten-Datenbank an. Wenn Sie das Replace-Argument verwenden, erstellt der Befehl import eine Tabelle für die Daten, die das neue Objekt in der Referenzdaten-Datenbank darstellt. Mit dem Befehl wird die von dem vorherigen Objekt identifizierte Tabelle nicht gelöscht.</p> <p>Um nicht verwendete Tabellen aus der Referenzdaten-Datenbank zu entfernen, führen Sie den Befehl infacmd cms Purge aus.</p>
-ImportType -it	Importtyp	Erforderlich. Der Typ des zu importierenden Inhalts. Geben Sie MetadataAndData für den Metadaten- und Datenimport ein.
-Folder -f	Der Ordner, aus dem importiert wird	Erforderlich für den Metadaten- und Datenimport. Vollständiger Pfad zu dem Ordner, der die zu importierende Referenzdatendatei enthält.
-FileName -fn	Nur für den Import eines einzelnen Wörterbuchs erforderlich	Erforderlich für den Import von Metadaten und Daten, wenn Sie Daten aus einer einzelnen Datei importieren. Name der Datei, die die gewünschten Referenzdaten zum Importieren enthält. Der Dateiname ist relativ zum Ordnerpfad.
-MetadataFile -mf	Nur für den Import von Objekten erforderlich	Erforderlich, wenn Sie nur Referenzdatenwerte importieren. Vollständiger Pfad und Name für die metadata.xml-Datei, auf die der Befehl angewendet werden soll. Die Datei „metadata.xml“ enthält die Metadaten, die mit den Referenzdatenwerten verknüpft sind. Nicht mit der Option ProjectFolder verwenden.
-ProjectFolder -pf	Name des Projektordners zum Importieren in	Erforderlich, wenn Sie Referenzdaten und Metadaten importieren. Name des Modellrepository-Projekts, in das Sie importieren möchten. Nicht mit der Option MetadataFile verwenden.
-NotRecursive -nr	- Unterordner nicht einbeziehen	Optional. Verwendung mit Metadaten- und Datenimport. Nur eine Objektebene importieren. Standardwert ist „rekursiv“.

# KAPITEL 33

## infacmd sch-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [CreateSchedule, 1130](#)
- [DeleteSchedule, 1137](#)
- [ListSchedule, 1138](#)
- [listScheduleOfUser, 1140](#)
- [ListServiceOptions, 1140](#)
- [ListServiceProcessOptions, 1141](#)
- [PauseAll, 1142](#)
- [PauseSchedule, 1143](#)
- [ResumeAll, 1144](#)
- [ResumeSchedule, 1145](#)
- [UpdateSchedule, 1146](#)
- [UpdateServiceOptions, 1149](#)
- [UpdateServiceProcessOptions, 1152](#)
- [updateUserPasswordInSchedule, 1155](#)
- [Upgrade, 1156](#)

### CreateSchedule

Erstellt einen Zeitplan für bereitgestellte Zuordnungen und bereitgestellte Workflows.

Der infacmd sch CreateSchedule-Befehl verwendet die folgende Syntax:

```
CreateSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ScheduleName|-scn> schedule_name

[<-ScheduleDescription|-scd> schedule_description]

<-Recurrence|-r> once|daily|weekly|monthly

<-StartTime|-st> yyyy-MM-dd HH:mm

[<-EndTime|-et> yyyy-MM-dd HH:mm]

[<-TimeZone|-tz> time_zone]

[<-DailyRunEvery|-dre> daily_run_every]

[<-RunDaysOfWeek|-rdw> mon|tue|wed|thu|fri|sat|sun]

[<-RunDayOfWeekMonth|-rdwm> monday|tuesday|wednesday|thursday|friday|saturday|sunday]

[<-RunDayOfMonth|-rdm> 1-30|LAST_DAY_OF_MONTH]

[<-RepeatCount|-rc> repeat_count]

[<-RunnableObjects|-ro> runnable_objects]

[<-Status|-ss> SCHEDULED|SUSPENDED]

[<-RunNow|-rn> true|false]

```

Zum Konfigurieren mehrerer Werte für ein Argument trennen Sie die Werte durch Kommas.

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch CreateSchedule“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-ScheduleName -scn	schedule_name	Erforderlich. Name des Zeitplans. Beim Namen des Zeitplans wird die Groß-/Kleinschreibung beachtet.

Option	Argument	Beschreibung
-Description -scd	schedule_description	Optional. Beschreibung des Zeitplans.
-Recurrence -r	once daily weekly monthly	Erforderlich. Geben Sie an, ob der Zeitplan einmal oder mehrmals ausgeführt wird.
-StartTime -st	yyyy-MM-dd HH:mm	Erforderlich. Datum und Uhrzeit des Beginns der Wiederholung.
-EndTime -et	yyyy-MM-dd HH:mm	Optional. Datum und Uhrzeit des Endes der Wiederholung.
-TimeZone -tz	Zeitzone	Optional. Zeitzone für den Anfangszeitpunkt des Zeitplans. Zum Konfigurieren der Zeitzone können Sie die ID-Nummer der Zeitzone oder die Olson-Datenbank-ID eingeben. Standardwert ist das Gebietsschema des Client-Computers.
-DailyRunEvery -dre	daily_run_every	Optional. Führen Sie den Zeitplan intervallweise aus. In der folgenden Liste werden die Optionen beschrieben, die Sie konfigurieren können: <ul style="list-style-type: none"> <li>- Minute(n). Führen Sie den Zeitplan täglich alle n Minuten aus.</li> <li>- Stunde(n). Führen Sie den Zeitplan täglich alle n Stunden aus.</li> <li>- Tag(e). Führen Sie den Zeitplan alle n Tage aus.</li> <li>- Woche(n). Führen Sie den Zeitplan alle n Wochen aus.</li> <li>- Monat(e). Führen Sie den Zeitplan alle n Monate aus.</li> <li>- Jahr(e). Führen Sie den Zeitplan alle n Jahre aus.</li> <li>- ERSTER. Führen Sie den Zeitplan an jedem ersten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben.</li> <li>- ZWEITER. Führen Sie den Zeitplan an jedem zweiten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben.</li> <li>- DRITTER. Führen Sie den Zeitplan an jedem dritten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben.</li> <li>- VIERTER. Führen Sie den Zeitplan an jedem vierten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben.</li> <li>- LETZTER. Führen Sie den Zeitplan an jedem letzten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben.</li> </ul>
-RunDaysOfWeek -rdw	mon tue wed thu fri sat sun	Optional. Führen Sie den Zeitplan an bestimmten Wochentagen aus.
-RunDayOfWeekMonth -rdwm	monday tuesday wednesday thursday friday saturday sunday	Optional. Führen Sie den Zeitplan monatlich an bestimmten Wochentagen aus. Verwenden Sie die Optionen -dre, um den Zeitplan alle ersten, zweiten, dritten, vierten oder letzten n-ten Tage des Monats auszuführen.
-RunDayOfMonth -rdm	1-30 LAST_DAY_OF_MONTH	Optional. Führen Sie den Zeitplan an Tag n des Monats aus.



Option	Argument	Beschreibung
-RepeatCount -rc	repeat_count	Optional. Beenden Sie die Wiederholung nach einer bestimmten Anzahl an Ausführungen statt an einem bestimmten Datum.
-RunnableObjects -ro	runnableObjects	<p>Optional. Objekte, die geplant werden sollen. Geben Sie den Objekttyp und dann den Pfad des Objekts im Datenintegrationsdienst an. Beispiel:</p> <pre>"workflow://DIS_hw2288/App_DMPA_run/wf_run_DMPA"</pre> <p>Optional können Sie die folgenden Argumente verwenden, um eine Parameterdatei, einen Parametersatz, das Ausführen als Benutzer oder ein Betriebssystemprofil für das Objekt zu konfigurieren:</p> <ul style="list-style-type: none"> <li>- parameterFilePath=PATH_TO_PARAMETER_FILE</li> <li>- parameterSet=PARAMETER_SET_NAME</li> <li>- runAsUser=USER_NAME     &amp;runAsUserSecurityDomain=SECURITY_DOMAIN     &amp;runAsUserPassword=PASSWORD</li> <li>- osProfileName=OS_PROFILE_NAME</li> </ul> <p>Beispiel:</p> <pre>"workflow:DIS_1234/Application_workflow/Workflow_abc? parameterFilePath=C://Informatica/Parameter Files/Parameter.xml &amp;runAsUser=Administrator &amp;runAsUserSecurityDomain=Native &amp;runAsUserPassword=Administrator"</pre>
-Status -ss	SCHEDULED PAUSED	Optional. Erstellen Sie den Zeitplan mit dem Status „Geplant“ oder „Angehalten“.
-RunNow -rn	true false	Führen Sie den Zeitplan sofort aus.

## Gültige Zeitzoneparameter

Wenn Sie den Zeitzoneparameter eingeben, können Sie eine Zeitzone-ID oder die Olson-Datenbank-ID eingeben.

In der folgenden Tabelle werden die Werte aufgelistet, die Sie für die Zeitzone eingeben können:

ID	Olson-Datenbank-ID	Name
0	Etc/GMT+12	(UTC-12:00) Internationale Datumsgrenze (Westen)
110	Etc/GMT+11	(UTC-11:00) Koordinierte Weltzeit-11
200	Pazifik/Honolulu	(UTC-10:00) Hawaii
300	Amerika/Anchorage	(UTC-09:00) Alaska

ID	Olson-Datenbank-ID	Name
410	Amerika/Santa_Isabel	(UTC-08:00) Baja California
400	Amerika/Los_Angeles	(UTC-08:00) PST (Pacific Standard Time – USA, Kanada)
520	Amerika/Phoenix	(UTC-07:00) Arizona
510	Amerika/Chihuahua	(UTC-07:00) Chihuahua, La Paz, Mazatlán
500	Amerika/Denver	(UTC-07:00) MST (Mountain Standard Time – USA, Kanada)
610	Amerika/Guatemala	(UTC-06:00) Mittelamerika
620	Amerika/Chicago	(UTC-06:00) CST (Central Standard Time – USA, Kanada)
630	Amerika/Mexico_City	(UTC-06:00) Guadalajara, Mexiko-Stadt, Monterrey
600	Amerika/Regina	(UTC-06:00) Saskatchewan
710	Amerika/Bogotá	(UTC-05:00) Bogotá, Lima, Quito, Rio Branco
700	Amerika/New_York	(UTC-05:00) EST (Eastern Standard Time – USA, Kanada)
720	Amerika/Indianapolis	(UTC-05:00) Indiana (Ost)
840	Amerika/Caracas	(UTC-04:30) Caracas
850	Amerika/Asunción	(UTC-04:00) Asunción
800	Amerika/Halifax	(UTC-04:00) AST (Atlantic Standard Time – Kanada)
810	Amerika/Cuiabá	(UTC-04:00) Cuiabá
830	Amerika/La_Paz	(UTC-04:00) Georgetown, La Paz, Manaus, San Juan
900	Amerika/St_Johns	(UTC-03:30) Neufundland
910	Amerika/Sao_Paulo	(UTC-03:00) Brasília
940	Amerika/Cayenne	(UTC-03:00) Cayenne, Fortaleza
950	Amerika/Buenos_Aires	(UTC-03:00) Buenos Aires Stadt
920	Amerika/Godthåb	(UTC-03:00) Grönland
930	Amerika/Montevideo	(UTC-03:00) Montevideo
820	Amerika/Santiago	(UTC-03:00) Santiago
1010	Etc/GMT+2	(UTC-02:00) Koordinierte Weltzeit-02
1100	Atlantik/Azoren	(UTC-01:00) Azoren

ID	Olson-Datenbank-ID	Name
1110	Atlantik/Cape_Verde	(UTC-01:00) Kapverdische Inseln
1220	Afrika/Casablanca	(UTC) Casablanca
1230	Etc/GMT	(UTC) Koordinierte Weltzeit
1200	Europa/London	(UTC) Dublin, Edinburgh, Lissabon, London
1210	Atlantik/Reykjavik	(UTC) Monrovia, Reykjavik
1340	Europa/Berlin	(UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
1300	Europa/Budapest	(UTC+01:00) Belgrad, Bratislava, Budapest, Ljubljana, Prag
1320	Europa/Paris	(UTC+01:00) Brüssel, Kopenhagen, Madrid, Paris
1310	Europa/Warschau	(UTC+01:00) Sarajevo, Skopje, Warschau, Zagreb
1330	Afrika/Lagos	(UTC+01:00) West-Zentralafrika
1350	Afrika/Windhuk	(UTC+01:00) Windhuk
1450	Asien/Amman	(UTC+02:00) Amman
1430	Europa/Bukarest	(UTC+02:00) Athen, Bukarest
1460	Asien/Beirut	(UTC+02:00) Beirut
1410	Afrika/Kairo	(UTC+02:00) Kairo
1480	Asien/Damaskus	(UTC+02:00) Damaskus
1470	Afrika/Johannesburg	(UTC+02:00) Harare, Pretoria
1420	Europa/Kiew	(UTC+02:00) Helsinki, Kiew, Riga, Sofia, Tallinn, Vilnius
1490	Europa/Istanbul	(UTC+02:00) Istanbul
1440	Asien/Jerusalem	(UTC+02:00) Jerusalem
1530	Europa/Kaliningrad	(UTC+02:00) Kaliningrad (RTZ 1)
1510	Asien/Bagdad	(UTC+03:00) Bagdad
1500	Asien/Riad	(UTC+03:00) Kuwait, Riad
1400	Europa/Minsk	(UTC+03:00) Minsk
1540	Europa/Moskau	(UTC+03:00) Moskau, St. Petersburg, Wolgograd (RTZ 2)
1520	Afrika/Nairobi	(UTC+03:00) Nairobi

ID	Olson-Datenbank-ID	Name
1550	Asien/Teheran	(UTC+03:30) Teheran
1600	Asien/Dubai	(UTC+04:00) Abu Dhabi, Muskat
1610	Asien/Baku	(UTC+04:00) Baku
1650	Indik/Mauritius	(UTC+04:00) Port Louis
1640	Asien/Tiflis	(UTC+04:00) Tiflis
1620	Asien/Eriwan	(UTC+04:00) Eriwan
1630	Asien/Kabul	(UTC+04:30) Kabul
1710	Asien/Taschkent	(UTC+05:00) Aschgabat, Taschkent
1700	Asien/Jekaterinburg	(UTC+05:00) Jekaterinburg (RTZ 4)
1750	Asien/Karatschi	(UTC+05:00) Islamabad, Karatschi
1720	Asien/Kalkutta	(UTC+05:30) Chennai, Kolkata, Mumbai, Neu-Delhi
1730	Asien/Colombo	(UTC+05:30) Sri Jayewardenepura
1740	Asien/Kathmandu	(UTC+05:45) Kathmandu
1800	Asien/Almaty	(UTC+06:00) Astana
1830	Asien/Dhaka	(UTC+06:00) Astana
1810	Asien/Nowosibirsk	(UTC+06:00) Nowosibirsk (RTZ 5)
1820	Asien/Rangun	(UTC+06:30) Yangon (Rangun)
1910	Asien/Bangkok	(UTC+07:00) Bangkok, Hanoi, Jakarta
1900	Asien/Krasnojarsk	(UTC+07:00) Krasnojarsk (RTZ 6)
2000	Asien/Schanghai	(UTC+08:00) Peking, Chongqing, Hongkong, Urumchi
2010	Asien/Irkutsk	(UTC+08:00) Irkutsk (RTZ 7)
2020	Asien/Singapur	(UTC+08:00) Kuala Lumpur, Singapur
2040	Australien/Perth	(UTC+08:00) Perth
2030	Asien/Taipeh	(UTC+08:00) Taipeh
2050	Asien/Ulan-Bator	(UTC+08:00) Ulan-Bator
2110	Asien/Tokio	(UTC+09:00) Osaka, Sapporo, Tokio
2100	Asien/Seoul	(UTC+09:00) Seoul

ID	Olson-Datenbank-ID	Name
2120	Asien/Jakutsk	(UTC+09:00) Jakutsk (RTZ 8)
2140	Australien/Adelaide	(UTC+09:30) Adelaide
2130	Australien/Darwin	(UTC+09:30) Darwin
2210	Australien/Brisbane	(UTC+10:00) Brisbane
2200	Australien/Sydney	(UTC+10:00) Canberra, Melbourne, Sydney
2240	Pazifik/Port_Moresby	(UTC+10:00) Guam, Port Moresby
2220	Australien/Hobart	(UTC+10:00) Hobart
2310	Asien/Magadan	(UTC+10:00) Magadan
2230	Asien/Wladiwostok	(UTC+10:00) Wladiwostok, Magadan (RTZ 9)
2300	Pazifik/Guadalcanal	(UTC+11:00) Salomonen, Neukaledonien
2410	Pazifik/Auckland	(UTC+12:00) Auckland, Wellington
2430	Etc/GMT-12	(UTC+12:00) Koordinierte Weltzeit+12
2400	Pazifik/Fidschi	(UTC+12:00) Fidschi
2500	Pazifik/Tongatapu	(UTC+13:00) Nuku'alofa
2510	Pazifik/Apia	(UTC+13:00) Samoa

## DeleteSchedule

Löscht einen oder mehrere Zeitpläne, die vom Scheduler-Dienst verwaltet werden.

Der infacmd sch DeleteSchedule-Befehl verwendet die folgende Syntax:

```

DeleteSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ScheduleName|-scn> schedule_name

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch DeleteSchedule“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-ScheduleName -scn	schedule_name	Name des zu löschenden Zeitplans.

## ListSchedule

Listet Zeitpläne oder geplante Objekte auf, die vom Scheduler-Dienst verwaltet werden. Der Befehl gibt Zeitpläne oder geplante Objekte zurück, die allen eingegebenen Optionen entsprechen.

Der infacmd sch ListSchedule-Befehl verwendet die folgende Syntax:

```
ListSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-ScheduleName|-scn> schedule_name]
[<-Description|-scd> description]
[<-RunnableObjects|-ro> runnable_objects]
[<-ScheduleStatus|-ss> created|scheduled|paused|complete]
[<-NumberOfFireTimes|-n> number_of_fire_times]
```

[<-MaxResults|-m> max\_results]

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListSchedule“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
ScheduleName -scn	schedule_name	Optional. Gibt Zeitpläne mit n Namen zurück.
Beschreibung -scd	Beschreibung	Optional. Gibt Zeitpläne mit n Beschreibungen zurück.
RunnableObjects -ro	runnableObjects	Optional. Listet die Zeitpläne auf, die ein Objekt ausführen. Geben Sie den Objekttyp und Pfad im Datenintegrationsdienst in folgendem Format ein:  '{mapping workflow}://dis_name/app_name/obj_name'  Beispiel:  'mapping://dis_demo/app_demo/mapping_demo'
ScheduleStatus -ss	created scheduled paused completed	Optional. Gibt Zeitpläne mit n Statusangaben zurück.
NumberOfFireTimes -n	number_of_fire_times	Optional. Gibt Zeitpläne zurück, die n Mal ausgeführt wurden.
Maxresults -m	max_results	Optional. Maximale Anzahl an Plänen, die vom Befehl zurückgegeben werden sollen.

# listScheduleOfUser

Lists all the scheduled jobs associated with a user.

The infacmd sch listScheduleOfUser command uses the following syntax:

```
listScheduleOfUser
<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-ScheduleUserName|-sun> schedules_of_user_name]
```

The following table describes infacmd sch listScheduleOfUser options and arguments:

Option	Argument	Description
-UserName -un	user_name	User name to connect to the Informatica domain.
-Password -pd	password	Password for the user.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-ScheduleUserName -sun	schedule_user_name	User name associated to the scheduled job. If you do not specify this value, the schedules are listed for the user specified in the -UserName option.

## ListServiceOptions

Gibt eine Liste mit den Eigenschaften zurück, die für den Scheduler-Dienst konfiguriert sind.

Der infacmd sch ListServiceOptions-Befehl verwendet die folgende Syntax:

```
ListServiceOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name
```



```

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch ListServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-ServiceName -sn	service_name	Erforderlich. Geben Sie Scheduler_Service ein.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.

## ListServiceProcessOptions

Gibt eine Liste mit den Eigenschaften zurück, die für einen Scheduler-Dienstprozess konfiguriert sind.

Der infacmd sch ListServiceProcessOptions-Befehl verwendet die folgende Syntax:

```

ListServiceProcessOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch ListServiceProcessOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-ServiceName -sn	service_name	Erforderlich. Geben Sie Scheduler_Service ein.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-NodeName -nn	node_name	Name des Knotens, auf dem der Dienstprozess ausgeführt wird.

## PauseAll

Hält alle Zeitpläne an, die vom Scheduler-Dienst verwaltet werden. Wenn Sie die Zeitpläne anhalten, werden bis zu deren Fortsetzung auch die in den Zeitplänen ausgeführten Objekte angehalten.

Der infacmd sch PauseAll-Befehl verwendet die folgende Syntax:

```
PauseAll  
<-DomainName|-dn> domain_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-SecurityDomain|-sdn> security_domain]  
  
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch PauseAll“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.

## PauseSchedule

Hält einen Zeitplan an, der vom Scheduler-Dienst verwaltet wird. Wenn Sie einen Zeitplan anhalten, werden bis zu dessen Fortsetzung auch die im Zeitplan ausgeführten Objekte angehalten.

Der infacmd sch PauseSchedule-Befehl verwendet die folgende Syntax:

```

PauseSchedule
<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ScheduleName|-scn> schedule_name

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch PauseSchedule“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-ScheduleName -scn	schedule_name	Name des Zeitplans, der angehalten werden soll. Beim Namen des Zeitplans wird die Groß-/Kleinschreibung beachtet.

## ResumeAll

Setzt alle angehaltenen Zeitpläne fort, die vom Scheduler-Dienst verwaltet werden.

Der infacmd sch ResumeAll-Befehl verwendet die folgende Syntax:

```
ResumeAll
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch ResumeAll“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.inf“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.

## ResumeSchedule

Setzt einen angehaltenen Zeitplan fort, der vom Scheduler-Dienst verwaltet wird.

Der infacmd sch ResumeSchedule-Befehl verwendet die folgende Syntax:

```
ResumeSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ScheduleName|-scn> schedule_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch ResumeSchedule“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
ScheduleName -scn	schedule_name	Name des angehaltenen Zeitplans, der fortgesetzt werden soll.

## UpdateSchedule

Aktualisiert einen Zeitplan, der vom Scheduler-Dienst verwaltet wird. Aktualisieren Sie einen Zeitplan, um die Start- oder Endzeiten, Wiederholungen oder Objekte zu ändern, die im Zeitplan ausgeführt werden. Führen Sie zum Anzeigen der aktuellen Optionen den infacmd sch ListSchedule-Befehl aus.

Der infacmd sch UpdateSchedule-Befehl verwendet die folgende Syntax:

```
UpdateSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ScheduleName|-scn> schedule_name
[<-ScheduleDescription|-scd> schedule_description]
<-Recurrence|-r> once|daily|weekly|monthly
<-StartTime|-st> yyyy-MM-dd HH:mm
```

```
[<-EndTime|-et> yyyy-MM-dd HH:mm]
[<-TimeZone|-tz> time_zone]
[<-DailyRunEvery|-dre> daily_run_every]
[<-RunDaysOfWeek|-rdw> mon|tue|wed|thu|fri|sat|sun]
[<-RunDayOfWeekMonth|-rdwm> monday|tuesday|wednesday|thursday|friday|saturday|sunday]
[<-RunDayOfMonth|-rdm> 1-30|LAST_DAY_OF_MONTH]
[<-RepeatCount|-rc> repeat_count]
[<-RemoveRunnableObjects|-rro> removeRunnableObjects]
[<-AddRunnableObjects|-aro> addRunnableObjects]
```

Zum Konfigurieren mehrerer Werte für ein Argument trennen Sie die Werte durch Kommas.

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch UpdateSchedule“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infra“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-ScheduleName -scn	schedule_name	Erforderlich. Name des Zeitplans. Beim Namen des Zeitplans wird die Groß-/Kleinschreibung beachtet.
-Description -scd	schedule_description	Optional. Beschreibung des Zeitplans.
-Recurrence -r	once daily weekly monthly	Erforderlich. Geben Sie an, ob der Zeitplan einmal oder mehrmals ausgeführt wird.
-StartTime -st	yyyy-MM-dd HH:mm	Erforderlich. Datum und Uhrzeit des Beginns der Wiederholung.
-EndTime -et	yyyy-MM-dd HH:mm	Optional. Datum und Uhrzeit des Endes der Wiederholung.

Option	Argument	Beschreibung
-TimeZone -tz	Zeitzone	Optional. Zeitzone für den Anfangszeitpunkt des Zeitplans. Zum Konfigurieren der Zeitzone können Sie die ID-Nummer der Zeitzone oder die Olson-Datenbank-ID eingeben. Standardwert ist das Gebietsschema des Client-Computers.
-DailyRunEvery -dre	daily_run_every	Optional. Führen Sie den Zeitplan intervallweise aus. In der folgenden Liste werden die Optionen beschrieben, die Sie konfigurieren können: <ul style="list-style-type: none"> <li>- Minute(n). Führen Sie den Zeitplan täglich alle n Minuten aus.</li> <li>- Stunde(n). Führen Sie den Zeitplan täglich alle n Stunden aus.</li> <li>- Tag(e). Führen Sie den Zeitplan alle n Tage aus.</li> <li>- Woche(n). Führen Sie den Zeitplan alle n Wochen aus.</li> <li>- Monat(e). Führen Sie den Zeitplan alle n Monate aus.</li> <li>- Jahr(e). Führen Sie den Zeitplan alle n Jahre aus.</li> <li>- ERSTER. Führen Sie den Zeitplan an jedem ersten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben.</li> <li>- ZWEITER. Führen Sie den Zeitplan an jedem zweiten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben.</li> <li>- DRITTER. Führen Sie den Zeitplan an jedem dritten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben.</li> <li>- Vierter. Führen Sie den Zeitplan an jedem vierten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben.</li> <li>- LETZTER. Führen Sie den Zeitplan an jedem letzten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben.</li> </ul>
-RunDaysOfWeek -rdw	mon tue wed thu fri sat sun	Optional. Führen Sie den Zeitplan an bestimmten Wochentagen aus.
-RunDayOfWeekMonth -rdwm	monday tuesday wednesday thursday friday saturday sunday	Optional. Führen Sie den Zeitplan monatlich an bestimmten Wochentagen aus. Verwenden Sie die Optionen -dre, um den Zeitplan alle ersten, zweiten, dritten, vierten oder letzten n-ten Tage des Monats auszuführen.
-RunDayOfMonth -rdm	1-30 LAST_DAY_OF_MONTH	Optional. Führen Sie den Zeitplan an Tag n des Monats aus.
-RepeatCount -rc	repeat_count	Optional. Beenden Sie die Wiederholung nach einer bestimmten Anzahl an Ausführungen statt an einem bestimmten Datum.



Option	Argument	Beschreibung
RemoveRunnableObjects -rro	removeRunnableObjects	Optional. Entfernt Objekte aus dem Zeitplan. Geben Sie Objekte in folgendem Format ein: <pre>"{mapping workflow}:Data Integration Service/ Application/{Mapping Workflow}[[?] [parameterFilePath=PATH_TO_PARAMETER_FILE  parameterSet=PARAMETER_SET_NAME] &amp;runAsUser=USER_NAME &amp;runAsUserSecurityDomain=SECURITY_DOMAIN &amp;runAsUserPassword=PASSWORD]]"</pre>
-AddRunnableObjects -aro	addRunnableObjects	Optional. Fügt dem Zeitplan Objekte hinzu. Objekte, die geplant werden sollen. Geben Sie den Objekttyp und dann den Pfad des Objekts im Datenintegrationsdienst an. Beispiel: <pre>"mapping:DIS_1234/Application_mapping/ Mapping_abc"</pre> Optional können Sie die folgenden Argumente verwenden, um eine Parameterdatei, einen Parametersatz, das Ausführen als Benutzer oder ein Betriebssystemprofil für das Objekt zu konfigurieren: <ul style="list-style-type: none"> <li>- parameterFilePath=PATH_TO_PARAMETER_FILE</li> <li>- parameterSet=PARAMETER_SET_NAME</li> <li>- runAsUser=USER_NAME  &amp;runAsUserSecurityDomain=SECURITY_DOMAIN  &amp;runAsUserPassword=PASSWORD</li> <li>- osProfileName=OS_PROFILE_NAME</li> </ul> Beispiel: <pre>"workflow:DIS_1234/Application_workflow/ Workflow_abc?parameterFilePath= C://Informatica/Parameter Files/Parameter.xml &amp;runAsUser=Administrator &amp;runAsUserSecurityDomain=Native &amp;runAsUserPassword=Administrator"</pre>

Eine Liste mit den gültigen Zeitzonewerten finden Sie unter ["Gültige Zeitzoneparameter" auf Seite 1133](#).

## UpdateServiceOptions

Aktualisiert die Eigenschaften für den Scheduler-Dienst. Führen Sie zum Anzeigen der aktuellen Optionen den `infacmd sch ListServiceOptions`-Befehl aus.

Der `infacmd sch UpdateServiceOptions`-Befehl verwendet die folgende Syntax:

```
UpdateServiceOptions
<-DomainName:-dn> domain_name
<-ServiceName|-sn> service_name
```

```

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-NodeName|-nn> primary node name]

[<-BackupNodes|-bn> node_name1,node_name2,...]

<-Options|-o> options

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch UpdateServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-ServiceName -sn	service_name	Erforderlich. Geben Sie Scheduler_Service ein.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
-NodeName -nn	Name des primären Knotens	Optional. Primärer Knoten, auf dem der Dienst ausgeführt wird.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist.
Optionen -o	options	Optional. Geben Sie jede Option durch ein Leerzeichen getrennt ein.

## Optionen des Scheduler-Diensts

Verwenden Sie die Optionen des Scheduler-Diensts mit dem `infacmd sch UpdateServiceOptions`-Befehl.

Geben Sie die Optionen des Scheduler-Diensts in folgendem Format ein:

```
... -o option_type.option_name=value
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Optionen des Scheduler-Diensts beschrieben:

Option	Beschreibung
<code>SchedulerPersistenceOptions.SchedulerRepositoryServiceName</code>	Der dem Scheduler-Dienst zugeordnete Modellrepository-Dienst.
<code>SchedulerPersistenceOptions.SchedulerRepositoryUsername</code>	Benutzername eines Administrator-Benutzers in der Informatica-Domäne. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.
<code>SchedulerPersistenceOptions.SchedulerRepositoryPassword</code>	Passwort des Administrator-Benutzers in der Informatica-Domäne. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.
<code>SchedulerPersistenceOptions.SchedulerRepositorySecurityDomain</code>	LDAP-Sicherheitsdomäne für den Benutzer, der den Scheduler-Dienst verwaltet. Das Sicherheitsdomänenfeld wird für Benutzer mit nativer oder Kerberos-Authentifizierung nicht angezeigt.

Option	Beschreibung
SchedulerLoggingOptions.SchedulerLogLevel	<p>Gibt den Standardschweregrad für die Dienstprotokolle an. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>- Schwerwiegend. Schreibt FATAL-Meldungen in das Protokoll. Zu FATAL-Meldungen gehören nicht behebbare Systemfehler, die bewirken, dass der Dienst beendet wird oder nicht mehr verfügbar ist.</li> <li>- Fehler. Schreibt FATAL- und ERROR-Codemeldungen in das Protokoll. Zu ERROR-Meldungen gehören Verbindungsfehler, Fehler beim Speichern oder Abrufen von Metadaten, Dienstfehler.</li> <li>- Warnung. Schreibt FATAL-, WARNING- und ERROR-Meldungen in das Protokoll. WARNING-Fehler beinhalten wiederherstellbare Systemfehler oder Warnungen.</li> <li>- Info. Schreibt FATAL-, INFO-, WARNING- und ERROR-Meldungen in das Protokoll. INFO-Meldungen beinhalten System- und Dienständerungsmeldungen.</li> <li>- Trace. Schreibt FATAL-, TRACE-, INFO-, WARNING- und ERROR-Meldungen in das Protokoll. In TRACE-Meldungen werden fehlerhafte Benutzeranfragen protokolliert.</li> <li>- Debug. Schreibt FATAL-, DEBUG-, TRACE-, INFO-, WARNING- und ERROR-Meldungen in das Protokoll. DEBUG-Meldungen sind Benutzeranfrageprotokolle.</li> </ul>
SchedulerStorageOptions.SchedulerTempFileLocation	<p>Pfad des Verzeichnisses, aus dem Parameterdateien gelesen und in das Parameterdateien geschrieben werden. Konfigurieren Sie für den Speicherort der temporären Dateien ein Verzeichnis, auf das alle Knoten in der Domäne zugreifen können.</p>

## UpdateServiceProcessOptions

Aktualisiert die Eigenschaften für einen Scheduler-Dienstprozess. Führen Sie zum Anzeigen der aktuellen Prozesskonfiguration den `infacmd sch ListServiceProcessOptions`-Befehl aus.

Der `infacmd sch UpdateServiceProcessOptions`-Befehl verwendet die folgende Syntax:

```
UpdateServiceProcessOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
[<-NodeName|-nn> node_name]
```

```
<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch UpdateServiceProcessOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-ServiceName -sn	service_name	Erforderlich. Geben Sie Scheduler_Service ein.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.
NodeName -nn	node_name	Name des Knotens, auf dem der Dienstprozess ausgeführt wird.
Optionen -o	options	Optional. Geben Sie jede Option durch ein Leerzeichen getrennt ein.

## Optionen des Scheduler-Dienstprozesses

Verwenden Sie die Optionen des Scheduler-Diensts mit dem infacmd sch UpdateServiceOptions-Befehl.

Geben Sie die Optionen des Scheduler-Diensts in folgendem Format ein:

```
... -o option_type.option_name=value
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Optionen des Scheduler-Diensts beschrieben:

Option	Beschreibung
SchedulerServiceAdvancedOptions.JVMOptions	<p>Java Virtual Machine (JVM)-Befehlszeilenooptionen zum Ausführen von Java-basierten Programmen. Bei der Konfiguration von JVM-Optionen müssen Sie die Eigenschaften für den Java SDK-Klassenpfad, den Java SDK-Minimalspeicher und den Java SDK-Maximalspeicher festlegen.</p> <p>Sie müssen die folgenden JVM-Befehlszeilenooptionen einstellen:</p> <ul style="list-style-type: none"> <li>- Xms. Minimale Heap-Größe. Standardwert ist 256 m.</li> <li>- MaxPermSize. Maximale permanente Generierungsgröße. Standardwert ist 128 m.</li> <li>- Dfile.encoding. Dateiverschlüsselung. Standardwert ist UTF-8.</li> </ul>
HttpConfigurationOptions.KeyStoreFile	<p>Pfad und Dateiname der Schlüsselspeicherdatei, die die Schlüssel und Zertifikate enthält. Erforderlich, wenn Sie HTTPS-Verbindungen für den Dienst verwenden. Sie können eine Schlüsselspeicherdatei mit einem Keytool erstellen. Bei Keytool handelt es sich um ein Dienstprogramm, das private oder öffentliche Schlüsselpaare und zugeordnete Zertifikate in einer Schlüsselspeicherdatei erzeugt und speichert. Sie können das selbstsignierte Zertifikat nutzen oder ein Zertifikat verwenden, das von einer Zertifizierungsstelle signiert wurde.</p>
HttpConfigurationOptions.KeyStorePassword	<p>Passwort für die Schlüsselspeicherdatei.</p>
HttpConfigurationOptions.TrustStoreFile	<p>Pfad und Dateiname der Truststore-Datei, die Authentifizierungszertifikate enthält, die vom Dienst als vertrauenswürdig eingestuft werden.</p>
HttpConfigurationOptions.TrustStorePassword	<p>Passwort für die Schlüsselspeicherdatei.</p>
HttpConfigurationOptions.SSLProtocol	<p>Zu verwendendes Secure Sockets Layer-Protokoll. Standardwert ist TLS.</p>
SchedulerServiceSecurityOptions.HttpPort	<p>Eindeutige HTTP-Portnummer für den Scheduler-Dienstprozess, wenn der Dienst das HTTP-Protokoll verwendet.</p> <p>Standardwert ist 6211.</p>
SchedulerServiceSecurityOptions.HttpsPort	<p>Eindeutige HTTPS-Portnummer für den Scheduler-Dienstprozess, wenn der Dienst das HTTPS-Protokoll verwendet.</p> <p>Wenn Sie eine HTTPS-Portnummer einrichten, müssen Sie auch die Schlüsselspeicherdatei definieren, die die erforderlichen Schlüssel und Zertifikate enthält.</p>

# updateUserPasswordInSchedule

When the password for a user is changed, the scheduled jobs associated with the user start to fail. The updateUserPasswordInSchedule command updates the password in the scheduler for a specified schedule name.

The infacmd sch updateUserPasswordInSchedule command uses the following syntax:

```
updateUserPasswordInSchedule
<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ScheduleName|-scn> schedule_name

[<-ScheduleUserName|-sun> schedule_user_name]

[<-ScheduleUserPassword|-sup> schedule_user_password]
```

The following table describes infacmd sch updateUserPasswordInSchedule options and arguments:

Option	Argument	Description
-UserName -un	user_name	User name to connect to the Informatica domain.
-Password -pd	password	Updated password for the user.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.inf file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-ScheduleName -scn	schedule_name	Name of the schedule for which you want to update the password.
-ScheduleUserName -sun	schedule_user_name	User name associated to the scheduled job. If you do not specify this value, -UserName is used to update the password.
-ScheduleUserPassword -sup	schedule_user_password	Updated password for the scheduler user. If you do not specify this value, -Password is used to update the password.

# Upgrade

Aktualisiert die Konfiguration des Scheduler-Diensts. Führen Sie „sch Upgrade“ aus, wenn Sie eine Aktualisierung auf die aktuelle Informatica-Version durchführen.

Der infacmd sch Upgrade-Befehl verwendet die folgende Syntax:

```
Upgrade
<-DomainName:-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch Upgrade“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne.
-ServiceName -sn	service_name	Erforderlich. Geben Sie Scheduler_Service ein.
-UserName -un	user_name	Benutzername zum Herstellen einer Verbindung zur Domäne.
-Password -pd	password	Das Passwort für den Benutzernamen.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen.



## KAPITEL 34

# infacmd search-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [CreateService, 1157](#)
- [ListServiceOptions, 1160](#)
- [ListServiceProcessOptions, 1162](#)
- [UpdateServiceOptions, 1164](#)
- [UpdateServiceProcessOptions, 1166](#)

## CreateService

Erstellt einen Suchdienst. Der Suchdienst wird standardmäßig aktiviert, wenn Sie ihn erstellen.

Der Befehl „infacmd search CreateService“ verwendet die folgende Syntax:

```
CreateService

<-DomainName|-dn> domain_name

<-NodeName|-nn> node_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-FolderPath|-fp> full_folder_path]

[<-BackupNodes|-bn> node_name1,node_name2,...]

<-SearchServicePort|-sp> search_service_port_number

<-IndexLocation|-il> search_index_location

<-ExtractionInterval|-ei> search_extraction_interval

<-RepositoryService|-rsn> model_repository_service_name

<-searchUserName|-sun> username_for_search_repositories

<-searchPassword|-spd> password_for_search_repositories
```

[<-searchSecurityDomain|-ssd> security\_domain\_of\_search\_repositories]

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd search CreateService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-NodeName -nn	node_name	Erforderlich. Knoten, auf dem der Suchdienst ausgeführt wird.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Suchdiensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codeseite des verbundenen Repositorys kompatibel sein. Der Name darf nicht länger als 230 Zeichen sein und keine Leerzeichen, Wagenrückläufe, Tabulatoren oder die folgenden Zeichen enthalten:  / * ? < > "
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad ohne den Domänennamen zu dem Ordner, zu dem Sie den Suchdienst hinzufügen möchten. Folgendes Format ist erforderlich: /parent_folder/child_folder Standardwert ist „/" (die Domäne).
-BackupNodes -bn	node_name1,node_name2,...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Sicherungsknoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.
-SearchServicePort -sp	search_service_port_number	Erforderlich. Port, auf dem der Suchdienst ausgeführt wird.
-IndexLocation -il	search_index_location	Das Verzeichnis, das die Suchindexdateien enthält.
-ExtractionInterval -ei	search_extraction_interval	Intervall in Sekunden, in dem der Suchdienst den Suchdienst aktualisiert.
-RepositoryService -rsn	model_repository_service_name	Modellrepository-Dienst für die Zuordnung zum Suchdienst. Der Modellrepository-Dienst kann keinem anderen Suchdienst zugeordnet werden.
-searchUserName -sun	username_for_search_repositories	Benutzername zum Zugriff auf den Modellrepository-Dienst. Der Modellrepository-Benutzer muss über die Administratorrolle verfügen.

Option	Argument	Beschreibung
-searchPassword -spd	password_for_search_repositories	Benutzerpasswort zum Zugriff auf den Modellrepository-Dienst.
-searchSecurityDomain -ssdn	security_domain_of_search_repositories	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu dem der Modellrepository-Benutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>

## ListServiceOptions

Listet die Eigenschaften für einen Suchdienst auf.

Der Befehl „`infacmd search ListServiceOptions`“ verwendet die folgende Syntax:

```
ListServiceOptions
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd search ListServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-NodeName -nn	node_name	Erforderlich. Knoten, auf dem der Suchdienst ausgeführt wird.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Suchdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## ListServiceProcessOptions

Listet die Eigenschaften für einen Suchdienstprozess auf.

Der Befehl „infacmd search ListServiceProcessOptions“ verwendet die folgende Syntax:

```
ListServiceProcessOptions
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd search ListServiceProcessOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienstprozess ausgeführt wird.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	Passwort	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-ServiceName -sn	service_name	Erforderlich. Name des Suchdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

# UpdateServiceOptions

Aktualisiert Suchdiensteigenschaften. Führen Sie zum Anzeigen der aktuellen Eigenschaften den `infacmd search ListServiceOptions`-Befehl aus.

Sie können die Eigenschaften ändern, während der Suchdienst ausgeführt wird. Sie müssen den Dienst jedoch recyceln, damit die Änderungen wirksam werden.

Der Befehl „`infacmd search UpdateServiceOptions`“ verwendet die folgende Syntax:

```
UpdateServiceOptions

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-Options|-o> options]

[<-NodeName|-nn> node_name]

[<-BackupNodes|-bn> node_name1,node_name2,...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd search UpdateServiceOptions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.



Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Suchdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Options -o	optionen	Optional. Geben Sie jede Option durch ein Leerzeichen getrennt ein. Setzen Sie einen Optionswert in doppelte Anführungszeichen, wenn er ein Leerzeichen enthält. Führen Sie zum Anzeigen der Optionen den infacmd search ListServiceOptions-Befehl aus.
-NodeName -nn	Name des Knotens	Optional. Knoten, auf dem dieser Suchdienst ausgeführt wird.
-BackupNodes -bn	node_name1,node_name2,.. ..	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Sicherungsknoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.

# UpdateServiceProcessOptions

Aktualisiert Eigenschaften für einen Suchdienstprozess. Führen Sie zum Anzeigen der aktuellen Eigenschaften den `infacmd search ListServiceProcessOptions`-Befehl aus.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Der Befehl „`infacmd search UpdateServiceProcessOptions`“ verwendet die folgende Syntax:

```
UpdateServiceProcessOptions
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd search UpdateServiceProcessOptions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
NodeName -nn	node_name	Erforderlich. Knoten, auf dem der Suchdienst ausgeführt wird.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	Passwort	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-ServiceName -sn	service_name	Erforderlich. Name des Suchdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-Options -o	optionen	<p>Erforderlich. Geben Sie jede Option durch ein Leerzeichen getrennt ein. Führen Sie zum Anzeigen der Optionen den infacmd search ListServiceProcessOptions-Befehl aus.</p>

# KAPITEL 35

## infacmd sql-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [ExecuteSQL, 1168](#)
- [ListColumnOptions, 1169](#)
- [ListColumnPermissions, 1171](#)
- [ListSQLDataServiceOptions, 1173](#)
- [ListSQLDataServicePermissions, 1175](#)
- [ListSQLDataServices, 1176](#)
- [ListStoredProcedurePermissions, 1178](#)
- [ListTableOptions, 1180](#)
- [ListTablePermissions, 1182](#)
- [PurgeTableCache, 1183](#)
- [RefreshTableCache, 1185](#)
- [RenameSQLDataService, 1187](#)
- [SetColumnPermissions, 1189](#)
- [SetSQLDataServicePermissions, 1191](#)
- [SetStoredProcedurePermissions, 1194](#)
- [SetTablePermissions, 1197](#)
- [StartSQLDataService, 1199](#)
- [StopSQLDataService, 1201](#)
- [UpdateColumnOptions, 1203](#)
- [UpdateSQLDataServiceOptions, 1206](#)
- [UpdateTableOptions, 1209](#)

## ExecuteSQL

Führt SQL-Anweisungen aus, die auf einen SQL-Datendienst zugreifen.

Führen Sie `infacmd sql ExecuteSQL` im interaktiven oder nicht interaktiven Modus aus. Wenn Sie `ExecuteSQL` im interaktiven Modus ausführen, können Sie SQL-Anweisungen eingeben, ohne ein Skript zu schreiben. Wenn Sie den interaktiven Modus verwenden, geben Sie den Verbindungsstring ohne die Option `-sql` ein. Sie können

nachfolgende SQL-Anweisungen ausführen, ohne die Verbindungsinformationen für jede Anweisung einzugeben.

Der Befehl `infacmd sql ExecuteSQL` verwendet die folgende Syntax:

```
ExecuteSQL
<-ConnectionString|-cs> connection_string
[<-Sql> sql_statement]
```

In der folgenden Tabelle werden die `infacmd sql ExecuteSQL`-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-ConnectionString -cs	connection_string	<p>Erforderlich. Geben Sie einen SQL-Datendienst-Verbindungsstring mit folgender Syntax ein:</p> <pre>jdbc:informatica:sqllds/ &lt;optional security domain\&gt; &lt;optional user name&gt;/ &lt;optional user password&gt;@ &lt;domain host name&gt;: &lt;domain HTTP port&gt;?dis= &lt;Data Integration Service name&gt;&amp;sqllds= &lt;runtime SQL data service name&gt;</pre> <p>Optional können Sie Optionen in folgendem Format hinzufügen:</p> <pre>... &amp;&lt;option_name&gt;=&lt;option_value&gt;</pre> <p>Der Verbindungsstring weist folgende Option und folgenden Wert auf:</p> <p><b>SQLDataServiceOptions.disableResultSetCache=true</b></p> <p>Deaktiviert das Ergebnissatz-Caching für eine SQL-Datendienstabfrage, wenn der SQL-Datendienst für das Caching des Ergebnissatzes konfiguriert ist.</p>
-Sql	sql_statement	Optional. Geben Sie eine SQL-Anweisung ein, wenn der interaktive Modus bei der Ausführung nicht verwendet werden soll.

## ListColumnOptions

Listet die Eigenschaften für Spalten in einer virtuellen Tabelle auf.

Der `infacmd sql ListColumnOptions`-Befehl verwendet die folgende Syntax:

```
ListColumnOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqllds> sql_data_service
<-Table|-t> schema.table
<-Column|-c> column
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql ListColumnOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendienstes.
-Table -t	schema.table	Erforderlich. Name der Tabelle. Definieren Sie die Tabelle mit der folgenden Syntax:  <schema_name>.<table_name>
-Column -c	column	Erforderlich. Name der Spalte.

## ListColumnPermissions

Listet Benutzer- und Gruppenberechtigungen für eine virtuelle Spalte auf.

Der Befehl „infacmd sql ListColumnPermissions“ verwendet die folgende Syntax:

```
ListColumnPermissions

<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-Table|-t> schema.table
<-Column|-c> column
<<-Direct> direct_permission_only|<-Effective> effective_permission_only>
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql ListTablePermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdienstes, auf dem die Anwendung bereitgestellt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeitdauer in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
SQLDataService -sqlds	sql_data_service	<p>Erforderlich. Name des SQL-Datendienstes.</p> <p>Sie müssen den Namen des SQL-Datendienstes zu dem Anwendungsnamen als Präfix hinzufügen.</p> <p>Verwenden Sie folgende Syntax:</p> <pre>&lt;application_name&gt;.&lt;SQL_data_service_name&gt;</pre>
-Table -t	schema.table	<p>Erforderlich. Name der Tabelle. Definieren Sie die Tabelle mit der folgenden Syntax:</p> <pre>&lt;schema_name&gt;.&lt;table_name&gt;</pre>



Option	Argument	Beschreibung
-Column -c	column	Erforderlich. Name der zu aktualisierenden Spalte.
-Direct   -Effective>	direct   effective	Erforderlich. Geben Sie entweder direct oder effective ein. Direkte Berechtigungen sind Berechtigungen, die dem Benutzer oder der Gruppe direkt zugewiesen werden. Effektive Berechtigungen umfassen direkte Berechtigungen und geerbte Berechtigungen.

## ListSQLDataServiceOptions

Listet die Eigenschaften eines SQL-Datendienstes auf, der in einem Datenintegrationsdienst bereitgestellt wird.

Der Befehl „`infacmd sql ListSQLDataServiceOptions`“ verwendet die folgende Syntax:

```
ListSQLDataServiceOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd sql ListSQLDataServiceOptions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-SQLDataService -sqls	sql_data_service	<p>Erforderlich. Name des SQL-Datendienstes.</p> <p>Sie müssen den Namen des SQL-Datendienstes zu dem Anwendungsnamen als Präfix hinzufügen.</p> <p>Verwenden Sie folgende Syntax:</p> <pre>&lt;application_name&gt;.&lt;SQL_data_service_name&gt;</pre>

# ListSQLDataServicePermissions

Listet die Berechtigungen für einen SQL-Datendienst auf.

Der Befehl „`infacmd sql ListSQLDataServicePermissions`“ verwendet die folgende Syntax:

```
ListSQLDataServicePermissions  
  
<-DomainName|-dn> domain_name  
  
<-ServiceName|-sn> service_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
[<-SecurityDomain|-sdn> security_domain]  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]  
  
<-SQLDataService|-sqlds> sql_data_service  
  
<<-Direct> direct_permission_only|<-Effective> effective_permission_only>
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd sql ListSQLDataServicePermissions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
SQLDataService -sqlds	sql_data_service	<p>Erforderlich. Name des SQL-Datendienstes.</p> <p>Sie müssen den Namen des SQL-Datendienstes zu dem Anwendungsnamen als Präfix hinzufügen.</p> <p>Verwenden Sie folgende Syntax:</p> <pre>&lt;application_name&gt;.&lt;SQL_data_service_name&gt;</pre>
-Direct   -Effective>	direct   effective	<p>Erforderlich. Ebene der aufzulistenden Berechtigungen. Direkte Berechtigungen sind Berechtigungen, die dem Benutzer oder der Gruppe direkt zugewiesen werden. Effektive Berechtigungen umfassen direkte Berechtigungen und geerbte Berechtigungen.</p>

## ListSQLDataServices

Listet die SQL-Datendienste für einen Datenintegrationsdienst auf.

Der Befehl „infacmd sql ListSQLDataServices“ verwendet die folgende Syntax:

```
ListSQLDataServices
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql ListSQLDataServices“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Datenintegrationsdienst, auf dem die Anwendung bereitgestellt wird.

## ListStoredProcedurePermissions

Listet die Berechtigungen für eine gespeicherte Prozedur auf.

Der Befehl „infacmd sql ListStoredProcedurePermissions“ verwendet die folgende Syntax:

```
ListStoredProcedurePermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-StoredProcedure|-sp> stored_procedure
<<-Direct> direct_permission_only|<-Effective> effective_permission_only>
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql ListStoredProcedurePermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
SQLDataService -sqlds	sql_data_service	<p>Erforderlich. Name des SQL-Datendienstes.</p> <p>Sie müssen den Namen des SQL-Datendienstes zu dem Anwendungsnamen als Präfix hinzufügen.</p> <p>Verwenden Sie folgende Syntax:</p> <pre>&lt;application_name&gt;.&lt;SQL_data_service_name&gt;</pre>

Option	Argument	Beschreibung
StoredProcedure -sp	stored_procedure	Erforderlich. Name der gespeicherten Prozedur.
-Direct   -Effective>	direct   effective	Erforderlich. Ebene der aufzulistenden Berechtigungen. Direkte Berechtigungen sind Berechtigungen, die dem Benutzer oder der Gruppe direkt zugewiesen werden. Effektive Berechtigungen umfassen direkte Berechtigungen und geerbte Berechtigungen.

## ListTableOptions

Listet die Eigenschaften für eine virtuelle Tabelle auf.

Der Befehl „`infacmd sql ListTableOptions`“ verwendet die folgende Syntax:

```
ListTableOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-Table|-t> schema.table
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd sql ListTableOptions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.



Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
SQLDataService -sqls	sql_data_service	<p>Erforderlich. Name des SQL-Datendienstes.</p> <p>Sie müssen den Namen des SQL-Datendienstes zu dem Anwendungsnamen als Präfix hinzufügen.</p> <p>Verwenden Sie folgende Syntax:</p> <pre>&lt;application_name&gt;.&lt;SQL_data_service_name&gt;</pre>
-Table -t	schema.table	<p>Erforderlich. Name der Tabelle. Definieren Sie die Tabelle mit der folgenden Syntax:</p> <pre>&lt;schema_name&gt;.&lt;table_name&gt;</pre>

# ListTablePermissions

Listet Gruppen- und Benutzerberechtigungen für eine virtuelle Tabelle auf.

Der Befehl „`infacmd sql ListTablePermissions`“ verwendet die folgende Syntax:

```
ListTablePermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SQLDataService|-sqlds> sql_data_service

<-Table|-t> schema.table

<-Direct> direct_permission_only|<-Effective> effective_permission_only>
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd sql ListTablePermissions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/ Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
SQLDataService -sqlds	sql_data_service	<p>Erforderlich. Name des SQL-Datendienstes.</p> <p>Sie müssen den Namen des SQL-Datendienstes zu dem Anwendungsnamen als Präfix hinzufügen.</p> <p>Verwenden Sie folgende Syntax:</p> <pre>&lt;application_name&gt;.&lt;SQL_data_service_name&gt;</pre>
-Table -t	schema.table	<p>Erforderlich. Name der Tabelle. Definieren Sie die Tabelle mit der folgenden Syntax:</p> <pre>&lt;schema_name&gt;.&lt;table_name&gt;</pre>
-Direct   -Effective>	direct   effective	Erforderlich. Geben Sie entweder direct oder effective ein. Direkte Berechtigungen sind Berechtigungen, die dem Benutzer oder der Gruppe direkt zugewiesen werden. Effektive Berechtigungen umfassen direkte Berechtigungen und geerbte Berechtigungen.

## PurgeTableCache

Bereinigt den Cache für virtuelle Tabellen.

Der Befehl „infacmd sql PurgeTableCache“ verwendet die folgende Syntax:

```
PurgeTableCache
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
```

```

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-SQLDataService|-sqlds> sql_data_service

<-Table|-t> table

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql PurgeTableCache“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendiensts. Sie müssen -sqlds als Präfix an den Anwendungsnamen anhängen. Verwenden Sie folgende Syntax: <application_name>.<SQL_data_service_name>
-Table -t	table	Erforderlich. Name des zu löschenden Cache für virtuelle Tabellen.

## RefreshTableCache

Aktualisiert den Cache eine virtuelle Tabelle.

Der Befehl „infacmd sql RefreshTableCache“ verwendet die folgende Syntax:

```
RefreshTableCache
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-SQLDataService|-sqlds> sql_data_service
<-Table|-t> table
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql RefreshTableCache“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

Option	Argument	Beschreibung
-SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendienstes. Sie müssen -sqlds als Präfix an den Anwendungsnamen anhängen. Verwenden Sie folgende Syntax: <application_name>.<SQL_data_service_name>
-Table -t	table	Erforderlich. Name des zu aktualisierenden Cache für virtuelle Tabellen.

## RenameSQLDataService

Benennt einen SQL-Datendienst um, der in einem Datenintegrationsdienst bereitgestellt wird.

Der Befehl „infacmd sql RenameSQLDataService“ verwendet die folgende Syntax:

```

RenameSQLDataService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-SQLDataService|-sqlds> sql_data_service
<-NewName|-n> new_name

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql RenameSQLDataService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem der SQL-Datendienst bereitgestellt wird.



Option	Argument	Beschreibung
-SQLDataService -sqlds	sql_data_service	Erforderlich. Name des umzubenennenden SQL-Datendienstes. Sie müssen den Namen des SQL-Datendienstes zu dem Anwendungsnamen als Präfix hinzufügen. Verwenden Sie folgende Syntax: <application_name>.<SQL_data_service_name>
NewItem -n	new_name	Erforderlich. Neuer Name für den SQL-Datendienst.

## SetColumnPermissions

Verweigert einer Gruppe oder einem Benutzer den Zugriff auf eine Spalte in einer SQL-Abfrage.

Der Befehl „infacmd sql SetColumnPermissions“ verwendet die folgende Syntax:

```
SetColumnPermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-Table|-t> schema.table
<-Column|-c> column_name
<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>
[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]
<-DeniedPermissions|-dp> denied_permissions
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql SetColumnPermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-SQLDataService -sqlds	sql_data_service	<p>Erforderlich. Name des SQL-Datendienstes mit der virtuellen Tabelle.</p> <p>Sie müssen den Namen des SQL-Datendienstes zu dem Anwendungsnamen als Präfix hinzufügen.</p> <p>Verwenden Sie folgende Syntax:</p> <pre>&lt;application_name&gt;.&lt;SQL_data_service_name&gt;</pre>

Option	Argument	Beschreibung
-Table -t	schema.table	Erforderlich. Name der virtuellen Tabelle. Geben Sie die Tabelle in folgendem Format ein:  <schema_name>.<table_name>
-Column -c	column	Name der zu aktualisierenden Spalte.
-GranteeUserName  GranteeGroupName -gun -ggn	grantee_user_name  grantee_group_name	Erforderlich. Benutzername bzw. Gruppenname, für den Berechtigungen festgelegt oder verweigert werden sollen.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, zu der der Benutzer gehört.
-DeniedPermissions -dp	denied_permissions	Erforderlich. Geben Sie „SQL_Select“ ein, um einen Benutzer daran zu hindern, die Spalte in eine SELECT-Anweisung aufzunehmen.

## SetSQLDataServicePermissions

Richtet die Gruppen- oder Benutzerberechtigungen für einen SQL-Datendienst ein. Sie können Berechtigungen auch verweigern.

Der Befehl „infacmd sql SetSQLDataServicePermissions“ verwendet die folgende Syntax:

```
SetSQLDataServicePermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>
[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]
<-AllowedPermissions|-ap> allowed_permissions
<-DeniedPermissions|-dp> denied_permissions
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd sql SetSQLDataServicePermissions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der <i>infacmd</i> versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendienstes. Sie müssen den Namen des SQL-Datendienstes zu dem Anwendungsnamen als Präfix hinzufügen. Verwenden Sie folgende Syntax: <code>&lt;application_name&gt;.&lt;SQL_data_service_name&gt;</code>
-GranteeUserName  GranteeGroupName -gun -ggn	grantee_user_name  grantee_group_name	Erforderlich. Benutzername bzw. Gruppenname, für den Berechtigungen festgelegt oder verweigert werden sollen.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, zu der der Benutzer gehört.
-AllowedPermissions -ap	allowed_permissions	Erforderlich. Liste der durch Leerzeichen getrennten Berechtigungen. Geben Sie eine der folgenden Berechtigungen ein: <ul style="list-style-type: none"> <li>- Grant. Benutzer können mithilfe des Administrator Tools oder des <i>infacmd</i>-Befehlszeilenprogramms Berechtigungen für den SQL-Datendienst gewähren oder widerrufen.</li> <li>- Execute. Benutzer können alle virtuellen gespeicherten Prozeduren im SQL-Datendienst mithilfe eines JDBC- oder ODBC-Client-Tools ausführen.</li> <li>- SQL_Select. Benutzer können SQL SELECT-Anweisungen in virtuellen Tabellen im SQL-Datendienst mithilfe eines JDBC- oder ODBC-Client-Tools ausführen.</li> </ul>
-DeniedPermissions -dp	denied_permissions	Optional. Liste der Berechtigungen, die Benutzern verweigert werden sollen. Trennen Sie jeden Parameter durch ein Leerzeichen. Geben Sie eine der folgenden Berechtigungen ein: <ul style="list-style-type: none"> <li>- EXECUTE. Benutzer können virtuell gespeicherte Prozeduren im SQL-Datendienst nicht ausführen.</li> <li>- SQL_SELECT. Benutzer können keine SELECT-Anweisungen in beliebigen Tabellen im SQL-Datendienst ausführen.</li> </ul>

# SetStoredProcedurePermissions

Richtet Benutzer- und Gruppenberechtigungen für eine gespeicherte Prozedur ein. Sie können Berechtigungen auch verweigern.

Der Befehl „`infacmd sql SetStoredProcedurePermissions`“ verwendet die folgende Syntax:

```
SetStoredProcedurePermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-StoredProcedure|-sp> stored_procedure
<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>
[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]
<-AllowedPermissions|-ap> allowed_permissions
<-DeniedPermissions|-dp> denied_permissions
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd sql SetStoredProcedurePermissions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendienstes mit der gespeicherten Prozedur.  Sie müssen den Namen des SQL-Datendienstes zu dem Anwendungsnamen als Präfix hinzufügen.  Verwenden Sie folgende Syntax: <code>&lt;application_name&gt;.&lt;SQL_data_service_name&gt;</code>
-StoredProcedure -sp	stored_procedure	Erforderlich. Name der gespeicherten Prozedur.
-GranteeUserName  GranteeGroupName -gun -ggn	grantee_user_name  grantee_group_name	Erforderlich. Benutzername bzw. Gruppenname, für den Berechtigungen festgelegt oder verweigert werden sollen.
- GranteeSecurityDomain -gsdn	grantee_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, zu der der Benutzer gehört.
-AllowedPermissions -ap	list_of_allowed_permissions_separated_by_space	Erforderlich. Liste der zulässigen Berechtigungen. Geben Sie einen der folgenden Parameter durch Leerzeichen getrennt ein: <ul style="list-style-type: none"> <li>- Grant. Benutzer können mithilfe des Administrator Tools oder des infacmd-Befehlszeilenprogramms Berechtigungen für die gespeicherten Prozedurobjekte gewähren oder widerrufen.</li> <li>- Execute. Benutzer können virtuelle gespeicherte Prozeduren im SQL-Datendienst mithilfe eines JDBC- oder ODBC-Client-Tools ausführen.</li> </ul>
-DeniedPermissions -dp	denied_permissions	Optional. Liste der Berechtigungen, die Benutzern verweigert werden sollen. Geben Sie einen der folgenden Parameter durch Leerzeichen getrennt ein: <ul style="list-style-type: none"> <li>- GRANT. Benutzer können Berechtigungen für die Objekte der gespeicherten Prozedur weder gewähren noch entziehen.</li> <li>- EXECUTE. Benutzer können keine gespeicherte Prozedur im SQL-Datendienst ausführen.</li> </ul>



# SetTablePermissions

Richtet Gruppen- und Benutzerberechtigungen für eine virtuelle Tabelle ein.

Der Befehl „infacmd sql SetTablePermissions“ verwendet die folgende Syntax:

```
SetTablePermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SQLDataService|-sqlds> sql_data_service

<-Table|-t> schema.table

<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>

[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]

<-AllowedPermissions|-ap> allowed_permissions

<-DeniedPermissions|-dp> denied_permissions

[<-RLSPredicate|-rls> row_level_security_predicate]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql SetTablePermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendienstes mit der virtuellen Tabelle.  Sie müssen den Namen des SQL-Datendienstes zu dem Anwendungsnamen als Präfix hinzufügen.  Verwenden Sie folgende Syntax:  <application_name>.<SQL_data_service_name>
-Table -t	schema.table	Erforderlich. Name der virtuellen Tabelle. Geben Sie die Tabelle in folgendem Format ein:  <schema_name>.<table_name>
-GranteeUserName  GranteeGroupName -gun -ggn	grantee_user_name  grantee_group_name	Erforderlich. Benutzername bzw. Gruppenname, für den Berechtigungen festgelegt oder verweigert werden sollen.

Option	Argument	Beschreibung
-GranteeSecurityDomain -gsdn	grantee_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, zu der der Benutzer gehört.
-AllowedPermissions -ap	list_of_allowed_permissions	Erforderlich. Liste der zulässigen Berechtigungen. Geben Sie einen der folgenden Parameter durch Leerzeichen getrennt ein: <ul style="list-style-type: none"> <li>- Grant. Benutzer können mithilfe des Administrator Tools oder des infacmd-Befehlszeilenprogramms Berechtigungen für die gespeicherten Prozedurobjekte gewähren oder widerrufen.</li> <li>- SQL_Select. Benutzer können SQL-Abfragen anhand der Tabelle durchführen.</li> </ul>
-DeniedPermissions -dp	denied_permissions	Optional. Liste der Berechtigungen, die Benutzern verweigert werden sollen. Geben Sie einen der folgenden Parameter durch Leerzeichen getrennt ein: <ul style="list-style-type: none"> <li>- GRANT. Benutzer können Berechtigungen für die Tabelle weder gewähren noch entziehen.</li> <li>- SQL_SELECT. Benutzer können keine SQL-Abfragen anhand der Tabelle durchführen.</li> </ul>
-RLSPredicate -rls	row_level_security_predicate	Optional. Listet das Sicherheitsprädikat auf Zeilenebene zum Anwenden auf SELECT-Anweisungen auf.

## StartSQLDataService

Startet einen SQL-Datendienst.

Der Befehl „infacmd sql StartSQLDataService“ verwendet die folgende Syntax:

```
StartSQLDataServiceOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql StartSQLDataService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendiensts. Sie müssen den Namen des SQL-Datendiensts zu dem Anwendungsnamen als Präfix hinzufügen. Verwenden Sie folgende Syntax: <application_name>.<SQL_data_service_name>

## StopSQLDataService

Hält die Ausführung eines SQL-Datendiensts an.

Der Befehl „infacmd sql StopSQLDataService“ verwendet die folgende Syntax:

```
StopSQLDataService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-SQLDataService|-sqlds> sql_data_service
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql StopSQLDataService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem der SQL-Datendienst bereitgestellt wird.
-SQLDataService -sqlds	sql_data_service	Erforderlich. Name des anzuhaltenden SQL-Datendienstes. Sie müssen den Namen des SQL-Datendienstes zu dem Anwendungsnamen als Präfix hinzufügen. Verwenden Sie folgende Syntax: <application_name>.<SQL_data_service_name>

## UpdateColumnOptions

Legt die Spaltenoptionen fest, um zu bestimmen, was beim Auswählen einer eingeschränkten Spalte in einer Abfrage geschieht. Sie können den Wert mit NULL oder mit einem konstanten Wert ersetzen.

Der Befehl „infacmd sql UpdateColumnOptions“ verwendet die folgende Syntax:

```
UpdateColumnOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-Table|-t> schema.table
<-Column|-c> column_name
<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql UpdateColumnOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-SQLDataService -sqlds	sql_data_service	<p>Erforderlich. Name des SQL-Datendienstes mit der virtuellen Tabelle.</p> <p>Sie müssen den Namen des SQL-Datendienstes zu dem Anwendungsnamen als Präfix hinzufügen.</p> <p>Verwenden Sie folgende Syntax:</p> <pre>&lt;application_name&gt;.&lt;SQL_data_service_name&gt;</pre>



Option	Argument	Beschreibung
-Table -t	schema.table	Erforderlich. Name der virtuellen Tabelle. Geben Sie die Tabelle in folgendem Format ein:  <schema_name>.<table_name>
-Column -c	column	Spaltenname.
-Options -o	options	Erforderlich. Geben Sie jede Option durch ein Leerzeichen getrennt ein. Führen Sie zum Anzeigen der aktuellen Optionen den infacmd sql ListColumnOptions-Befehl aus.

## Spaltenoptionen

Verwenden Sie Spaltenoptionen zum Aktualisieren einer Spalte. Verwenden Sie die Spaltenoptionen mit dem Befehl `infacmd sql UpdateColumnOptions`.

Geben Sie die Spaltenoptionen in folgendem Format ein:

```
... -o UpdateColumnOptions.option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden Spaltenoptionen beschrieben:

Optionen	Beschreibung
ColumnOptions.DenyWith	Wenn Sie Sicherheit auf Spaltenebene verwenden, bestimmt diese Eigenschaft, ob die Abfrage fehlschlagen oder der Wert der eingeschränkten Spalte ersetzt werden soll. Sie können den Spaltenwert durch NULL oder einen konstanten Wert ersetzen. Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none"> <li>- ERROR. Lässt die Abfrage fehlschlagen und gibt einen Fehler zurück.</li> <li>- NULL. Gibt Nullwerte für eine eingeschränkte Spalte in jeder Zeile zurück.</li> <li>- VALUE. Gibt einen konstanten Wert anstelle der eingeschränkten Spalte in jeder Zeile zurück. Konfigurieren Sie den konstanten Wert in der Option <code>InsufficientPermissionValue</code>.</li> </ul>
ColumnOptions.InsufficientPermissionValue	Ersetzt den Wert der eingeschränkten Spalte durch einen konstanten Wert. Der Standardwert ist ein leerer String. Wenn Sie <code>ColumnOptions.DenyWith</code> nicht konfigurieren, ignoriert der Data Integration Service die Option <code>InsufficientPermissionValue</code> .

# UpdateSQLDataServiceOptions

Aktualisiert SQL-Datendienst-Eigenschaften. Sie müssen vor dem Aktualisieren der Eigenschaften den SQL-Datendienst beenden.

Der Befehl „`infacmd sql UpdateSQLDataServiceOptions`“ verwendet die folgende Syntax:

```
UpdateSQLDataServiceOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd sql UpdateSQLDataServiceOptions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-SQLDataService -sqlds	sql_data_service	<p>Erforderlich. Name des SQL-Datendienstes.</p> <p>Sie müssen den Namen des SQL-Datendienstes zu dem Anwendungsnamen als Präfix hinzufügen.</p> <p>Verwenden Sie folgende Syntax:</p> <pre>&lt;application_name&gt;.&lt;SQL_data_service_name&gt;</pre>
options -o	options	<p>Erforderlich. Liste der zu aktualisierenden Optionen. Geben Sie Optionen und Werte durch Leerzeichen getrennt ein. Führen Sie zum Anzeigen der Optionen für einen SQL-Datendienst infacmd sql ListSQLDataServiceOptions aus.</p>

## SQL-Datendienst-Optionen

Verwenden Sie SQL-Datendienst-Optionen zum Aktualisieren eines SQL-Datendienstes. Verwenden Sie SQL-Datendienst-Optionen mit dem Befehl `infacmd sql UpdateSQLDataServiceOptions`.

Geben Sie SQL-Datendienst-Optionen in folgendem Format ein:

```
... -o SQLDataServiceOptions.option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden Verbindungsoptionen für `infacmd sql UpdateSQLDataServiceOptions` beschrieben:

Option	Beschreibung
<code>SQLDataServiceOptions.startupType</code>	Legt fest, ob der SQL-Datendienst beim Starten der Anwendung oder des SQL-Datendienstes zur Ausführung aktiviert ist. Geben Sie <code>ENABLED</code> ein, damit der SQL-Datendienst ausgeführt wird. Geben Sie <code>DISABLED</code> ein, damit der SQL-Datendienst nicht ausgeführt wird.
<code>SQLDataServiceOptions.traceLevel</code>	Ebene der in das Sitzungsprotokoll geschriebenen Fehlermeldungen. Geben Sie eine der folgenden Meldungsebenen an: <ul style="list-style-type: none"> <li>- Schwerwiegend</li> <li>- Fehler</li> <li>- Info</li> <li>- Trace</li> <li>- Debug</li> </ul>
<code>SQLDataServiceOptions.connectionTimeout</code>	Maximale Anzahl an Millisekunden, in denen auf eine Verbindung zum SQL-Datendienst gewartet wird. Standardwert ist 3.600.000.
<code>SQLDataServiceOptions.requestTimeout</code>	Maximale Anzahl an Millisekunden, in denen bei einer SQL-Anfrage auf eine Antwort vom SQL-Datendienst gewartet wird. Standardwert ist 3.600.000.
<code>SQLDataServiceOptions.sortOrder</code>	Sortierreihenfolge, die der Data Integration Service zum Sortieren und Vergleichen von Daten verwendet, wenn er im Unicode-Modus ausgeführt wird. Sie können die Sortierreihenfolge basierend auf Ihrer Codeseite auswählen. Wenn der Data Integration Service im ASCII-Modus ausgeführt wird, ignoriert er den Sortierreihenfolgenwert und verwendet eine binäre Sortierreihenfolge. Die Standardeinstellung ist "binär".
<code>SQLDataServiceOptions.maxActiveConnections</code>	Maximale Anzahl an aktiven Verbindungen zum SQL-Datendienst. Standardwert ist 10.
<code>SQLDataServiceOptions.ResultSetCacheExpirationPeriod</code>	Die Anzahl an Millisekunden, die der Ergebnissatz-Cache verwendet werden kann. Wenn der Wert auf -1 festgelegt ist, läuft der Cache nie ab. Wenn der Wert auf 0 festgelegt ist, ist das Ergebnissatz-Caching deaktiviert. Änderungen des Ablaufzeitraums gelten nicht für vorhandene Caches. Wenn alle Caches denselben Ablaufzeitraum verwenden sollen, bereinigen Sie den Ergebnissatz-Cache, nachdem Sie den Ablaufzeitraum geändert haben. Standardwert ist 0.

Option	Beschreibung
SQLDataServiceOptions.DTMKeepAliveTime	Anzahl der Millisekunden, für die die DTM-Instanz geöffnet bleibt, nachdem sie die letzte Anfrage abgeschlossen hat. Identische SQL-Abfragen können die offene Instanz wiederverwenden. Verwenden Sie die Keep Alive-Zeit, um die Leistung zu erhöhen, wenn die für die Verarbeitung der SQL-Abfrage erforderliche Zeit im Vergleich zur Dauer der Initialisierung der DTM-Instanz gering ist. Wenn die Abfrage fehlschlägt, wird die DTM-Instanz beendet. Muss eine Ganzzahl sein. Eine negative Ganzzahl bedeutet, dass die DTM-Keep Alive-Zeit für den Data Integration Service verwendet wird. 0 bedeutet, dass der Data Integration Service die DTM-Instanz nicht im Speicher beibehält. Standardwert ist -1.
SQLDataServiceOptions.optimizeLevel	Die Optimierungsebene, die der Data Integration Service für das Objekt anwendet. Geben Sie den numerischen Wert ein, der mit der Optimierungsebene verbunden ist, die Sie konfigurieren möchten. Sie können Sie einen der folgenden numerischen Werte eingeben: <ul style="list-style-type: none"> <li>- 0. Der Datenintegrationsdienst wendet keine Optimierung an.</li> <li>- 1. Der Datenintegrationsdienst wendet die frühe Projektionsoptimierungsmethode an.</li> <li>- 2. Der Datenintegrationsdienst wendet die Optimierungsmethoden „Frühe Projektion“, „Frühe Auswahl“, „Push-Into“ und „Prädikat“ an.</li> <li>- 3. Der Datenintegrationsdienst wendet die Optimierungsmethoden „Kostenbasiert“, „Frühe Projektion“, „Frühe Auswahl“, „Push-Into“, „Prädikat“ und „Semi-Join“ an.</li> </ul>

## UpdateTableOptions

Aktualisiert die virtuellen Tabelleneigenschaften. Sie müssen vor dem Aktualisieren der Eigenschaften den SQL-Datendienst beenden.

Der Befehl „infacmd sql UpdateTableOptions“ verwendet die folgende Syntax:

```
UpdateTableOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-Table|-t> schema.table
<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql UpdateTableOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendienstes. Sie müssen den Namen des SQL-Datendienstes zu dem Anwendungsnamen als Präfix hinzufügen. Verwenden Sie folgende Syntax: <application_name>.<SQL_data_service_name>
-Table -t	schema.table	Erforderlich. Name der Tabelle. Verwenden Sie folgende Syntax: <schema_name>.<table_name>
Options -o	options	Erforderlich. Geben Sie das Name-Wert-Paar durch Leerzeichen getrennt ein.

## Virtuelle Tabellenoptionen

Verwenden Sie die virtuellen Tabellenoptionen, um das Zwischenspeichern für eine virtuelle Tabelle zu konfigurieren. Verwenden Sie die virtuellen Tabellenoptionen mit dem `infacmd sql UpdateTableOptions`-Befehl.

Geben Sie virtuelle Tabellenoptionen im folgenden Format ein:

```
... -o option_type.option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Die folgende Tabelle beschreibt die virtuellen Tabellenoptionen:

Option	Beschreibung
VirtualTableOptions.CachingEnabled	Zwischenspeichern der virtuellen Tabelle in der Cache-Datenbank des Datenobjekts. „True“ oder „False“. Standardwert ist „True“.
VirtualTableOptions.CacheRefreshPeriod	Anzahl der Minuten zwischen den Cache-Aktualisierungen. Standardwert ist Null.
VirtualTableOptions.CacheTableName	Der Name der benutzerverwalteten Tabelle, aus der der Datenintegrationsdienst auf den Cache der virtuellen Tabelle zugreift. Eine benutzerverwaltete Cache-Tabelle ist eine Tabelle in der Cache-Datenbank des Datenobjekts, die Sie bei Bedarf erstellen, füllen und manuell aktualisieren können.  Wenn Sie einen Cache-Tabellennamen angeben, verwaltet der Datenobjekt-Cache-Manager den Cache für das Objekt nicht und ignoriert den Cache-Aktualisierungszeitraum. Wenn Sie keinen Cache-Tabellennamen angeben, verwaltet der Datenobjekt-Cache-Manager den Cache für das Objekt.

## KAPITEL 36

# infacmd tdm-Befehlsreferenz

Der Test Data Manager-Dienst wird über das *infacmd* tdm-Programm verwaltet.

Mit den *infacmd* tdm-Befehlen können Sie den Dienst erstellen, Inhalt zum Dienst hinzufügen und den Dienst aktivieren bzw. deaktivieren.

## CreateService

Erstellt einen Test Data Manager-Dienst in einer Domäne.

Der Befehl „*infacmd tdm CreateService*“ verwendet die folgende Syntax:

```
CreateService
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
<-LicenseName|-ln> license_name

<-MRSServiceName|-mrs> model_repo_service
<-MRSUserName|-rsun> model_repo_service_username
<-MRSPassword|-rspd> model_repo_service_password
[<-MRSSecurityDomain|-rsdn> model_repo_security_domain]

<-EnableProfiling|-ep> enable_profiling

<-DISServiceName|-dis> data_integration_service
<-db_type|-dt> database_type (ORACLE, DB2, SQLSERVER or CUSTOM)
<-DBUsername|-du> db_user
<-DBPassword|-dp> db_password
```



```

<-DBUrl|-dl> db_url
<-DBConnectionString|-dc> db_conn_string
[<-DbSchema|-ds> db_schema (used for SQL Server only)]
[<-DbTablespace|-db> db_tablespace (used for DB2 only)]
[<-HttpPort> http_port]
[<-HttpsPort> https_port]
[<-KeystoreFile|-kf> keystore_file_location]
[<-KeystorePassword|-kp> keystore_password]
[<-SSLProtocol|-sp> ssl_protocol]
[<-jvmParams|-jp> jvmParameters]
[<-connPoolSize|-cp> conn_pool_size]
[<-jmxPort> jmx_port]
[<-shutdownPort> shutdown_port]
[<-hadoopDistDir> Hadoop Distribution Directory]
[<-hadoopKerbSPN> Hadoop Kerberos Service Principal Name]
[<-hadoopKerbKeytab> Hadoop Kerberos Keytab]

```

In der folgenden Tabelle werden „infacmd tdm CreateService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Test Data Manager-Diensts.  Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositories kompatibel sein. Der Name darf maximal 230 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten:  / * ? < > "

Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänenennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang. Standardwert ist 180 Sekunden.

Option	Argument	Beschreibung
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienst ausgeführt wird.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten: / * ? < > "
-MRSServiceName -mrs	model_repo_service	Name des Modellrepository-Diensts, mit dem sich TDM verbindet.
-MRSUserName -rsun	model_repo_service_username	Erforderlich. Benutzername für die Verbindung zum Modellrepository.
-MRSPassword -rspd	model_repo_service_password	Erforderlich. Passwort für den Benutzernamen zur Verbindung mit dem Modellrepository. Beim Passwort wird die Groß-/Kleinschreibung beachtet.
-MRSSecurityDomain -rsdn	model_repo_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Native“.
-EnableProfiling -ep	enable_profiling	Gibt Einstellungen für die Datenerkennung an. Auf TRUE festlegen, um die Datenerkennung zu aktivieren. Auf FALSE festlegen, um die Datenerkennung zu deaktivieren.
-DISServiceName -dis	data_integration_service	Name des Datenintegrationsdiensts, mit dem sich TDM verbindet.
-db_type -dt	database_type	Typ der TDM-Repository-Datenbank. Werte sind „Oracle“, „SQL Server“, „DB2“ oder „Benutzerdefiniert“.
-DBUsername -du	db_user	Erforderlich. Konto für die Repository-Datenbank. Verwenden Sie den Datenbank-Client, um dieses Konto einzurichten.
-DBPassword -dp	db_password	Erforderlich. Passwort der Repository-Datenbank für den Datenbankbenutzer.

Option	Argument	Beschreibung
-DBUrl -dl	db_url	<p>Erforderlich. JDBC-Verbindungszeichenfolge zur Datenbank für das TDM-Repository. Verwenden Sie eine der folgenden Syntaxen:</p> <p><b>Oracle:</b></p> <pre>jdbc:informatica:oracle: // &lt;machineName&gt;:&lt;PortNo&gt;;ServiceName= &lt;DBName&gt;; MaxPooledStatements=20; CatalogOptions=0; EnableServerResultCache=true</pre> <p><b>DB2:</b></p> <pre>jdbc:informatica:db2: //&lt;host&gt;:&lt;port&gt;; DatabaseName=&lt;dbname&gt;; BatchPerformanceWorkaround=true;Dynam icSections=1000</pre> <p><b>SQLServer:</b></p> <pre>jdbc:informatica:sqlserver: // &lt;host&gt;:&lt;port&gt;; DatabaseName=&lt;dbname&gt;; SnapshotSerializable=true</pre>
-DBConnString -dc	db_conn_string	Native Verbindungszeichenfolge für die TDM-Repository-Datenbank. Der Dienst verwendet die Verbindungszeichenfolge, um ein Verbindungsobjekt für das Test Data Manager- und das PowerCenter- oder Modellrepository zu erstellen.
-DbSchema -ds	db_schema	Optional. Der Schemaname für eine Microsoft SQL Server-Datenbank.
-DbTablespace -db	db_tablespace	<p>Nur für eine DB2-Datenbank erforderlich. Beim Konfigurieren eines Tablespace-Namens erstellt der Test Data Manager-Dienst alle Repository-Tabellen im selben Tablespace. Sie können im Tablespace-Namen keine Leerzeichen verwenden.</p> <p>Der Tablespace muss auf einem Einzelknoten definiert werden und die Seitengröße muss 32 KB betragen. In einer Datenbank mit mehreren Partitionen müssen Sie diese Option auswählen. Wenn Sie in einer Datenbank mit einer Partition diese Option nicht auswählen, erstellt das Installationsprogramm die Tabellen im Standard-Tablespace.</p>
-HttpPort	http_port	Erforderlich. Portnummer des Diensts.
-HttpsPort	https_port	Optional. Portnummer zum Sichern der Verbindung zum Administrator Tool. Geben Sie diese Portnummer an, wenn Sie HTTPS für einen Knoten konfigurieren möchten.
-KeystoreFile -kf	keystore_file_location]	Optional. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die bei Verwendung des SSL-Protokolls mit PowerCenter erforderlich sind.

Option	Argument	Beschreibung
-KeystorePassword -kp	keystore_password	Optional. Wenn TLS aktiviert ist, müssen Sie ein Passwort festlegen.
-SSLProtocol -pt	SSL-Protokoll	Optional. Zu verwendendes Secure Sockets Layer-Protokoll. Kann bei Aktivierung von TLS (Transport Layer Security) bearbeitet werden.
-jvmParams -jp	jvmParameters	<p>Festzulegende JVM-Parameter:</p> <ul style="list-style-type: none"> <li>- Die Test Data Manager zugeordnete Heap-Größe.</li> <li>- Der Zeitraum, nach dessen Ablauf Datenbankverbindungen erneuert werden, wenn sich die TDM-Benutzeroberfläche weiterhin im Leerlauf befindet. Erforderlich, wenn Sie die Konfigurationseinstellungen der Datenbank in niedrigere Werte als die TDM-Standardwerte geändert haben. Bearbeiten Sie die Werte in TDM so, dass die Werte niedriger als die Datenbankwerte sind.</li> </ul> <p>Schließen Sie die JVM-Parameter in einfache Anführungszeichen und anschließend in doppelte Anführungszeichen ein. Beispiel: 'value' und dann "value".</p> <p>Die Option -Xms unterscheidet zwischen Groß- und Kleinschreibung. Beispiel:</p> <p>"" - Xms512m - Xmx1024m - XX:MaxPermSize=512m"</p> <ul style="list-style-type: none"> <li>- IDLE_TIME.</li> <li>-DIDLE_TIME=&lt;seconds&gt;. Standardwert ist 300 Sekunden.</li> <li>- CONNECT_TIME.</li> <li>-DCONNECT_TIME=&lt;seconds&gt;. Standardwert ist 5000 Sekunden.</li> </ul>
-connPoolSize -cp	conn_pool_size	Optional. Die maximale Anzahl inaktiver Verbindungsinstanzen, die ein Pool für eine Datenbankverbindung aufrechterhält, bevor die maximale inaktive Zeit erreicht ist. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Standardwert ist 15.
-jmxPort	jmx_port	Portnummer für die JMX/RMI-Verbindungen mit TDM. Standardwert ist 6675.
-shutdownPort	shutdown_port	Portnummer, die das Herunterfahren von TDM steuert.
-hadoopDistDir -hdd	Hadoop-Distributionsverzeichnis	Das Hadoop-Distributionsverzeichnis auf dem Test Data Manager-Dienstknoten.

Option	Argument	Beschreibung
-hadoopKerbSPN -hks	Hadoop-Kerberos-Dienstprinzipalname	Dienstprinzipalname (SPN) des Datenintegrationsdiensts zum Herstellen einer Verbindung zu einem Hadoop-Cluster, der Kerberos-Authentifizierung verwendet. Nicht erforderlich, wenn Sie die MapR Hadoop-Distribution ausführen. Für andere Hadoop-Distributionen erforderlich.
-hadoopKerbKeytab -hkt	Hadoop-Kerberos-Keytab	Der Dateipfad der Kerberos-Keytab-Datei auf dem Computer, auf dem der Datenintegrationsdienst ausgeführt wird. Nicht erforderlich, wenn Sie die MapR Hadoop-Distribution ausführen. Für andere Hadoop-Distributionen erforderlich.

## CreateContents

Erstellt den Repository-Inhalt für das Test Data Manager-Repository.

Der Befehl „`infacmd tdm CreateContents`“ verwendet die folgende Syntax:

```
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd tdm CreateContents“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Der Name des Test Data Manager-Diensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## EnableService

Aktiviert den Test Data Manager-Dienst.

Der Befehl „infacmd tdm EnableService“ verwendet die folgende Syntax:

```
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd idm EnableService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, zu dem Sie den Befehl ausführen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.



Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

## DisableService

Deaktiviert den Test Data Manager-Dienst. Wenn Sie den Test Data Manager-Dienst deaktivieren, werden alle Dienstprozesse angehalten.

Der Befehl „infacmd tdm DisableService“ verwendet die folgende Syntax:

```
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
```

```

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-DisableMode|-dm> disable_mode: COMPLETE|ABORT|STOP

```

In der folgenden Tabelle werden „infacmd tdm DisableService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, zu dem Sie den Befehl ausführen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_se conds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-DisableMode -dm	disable_mode	Erforderlich. Definiert, wie der Dienst deaktiviert wird: <ul style="list-style-type: none"> <li>- Vollständig. Deaktiviert den Dienst, nachdem alle Dienstprozesse gestoppt sind.</li> <li>- Abbrechen. Stoppt alle Prozesse sofort und deaktiviert dann den Dienst.</li> <li>- Stoppen. Stoppt alle laufenden Arbeitsabläufe und deaktiviert dann den Dienst.</li> </ul>

## KAPITEL 37

# infacmd tools-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [deployApplication, 1224](#)
- [exportObjects, 1226](#)
- [exportResources, 1228](#)
- [importObjects, 1230](#)
- [patchApplication, 1234](#)

## deployApplication

Stellt eine Anwendung in einer .iar-Datei bereit.

Stellen Sie eine Anwendung in einer Datei bereit, wenn die Anwendung eine große Anzahl von Objekten enthält. Führen Sie im Anschluss an den Befehl „infacmd tools deployApplication“ den Befehl „infacmd dis deployApplication“ aus, um die Anwendung für einen Datenintegrationsdienst bereitzustellen.

Der Befehl „infacmd tools deployApplication“ verwendet folgende Syntax:

```
deployApplication
<-DomainName|-dn> Domain name
<-UserName|-un> User name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> Security domain]
<-RepositoryService|-rs> Model Repository Service name
<-OutputDirectory|-od> Output directory
<-ApplicationPath|-ap> Application path
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd tools deployApplication“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	Domänenname	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-RepositoryService -rs	Name des Modellrepository-Diensts	Erforderlich. Name des Modellrepository-Diensts.

Option	Argument	Beschreibung
- OutputDirectory -od	Ausgabeverzeichnis	Erforderlich. Verzeichnis, in das die IAR-Datei geschrieben werden soll.
-ApplicationPath -ap	Anwendungspfad	Erforderlich. Der Anwendungspfad, beginnend mit den Projektnamen, Ordernamen und gefolgt vom Namen der Anwendung. Trennen Sie den Projektnamen, Ordernamen und den Namen der Anwendung mit einem Schrägstrich (/). Beispiel: „Projekt/Ordner1/Ordner2/Anwendung“.

## exportObjects

Exportiert Objekte aus einem Projekt im Modellrepository in eine XML-Datei.

Wenn Sie nicht alle Objekte im Projekt exportieren möchten, verwenden Sie eine infacmd-Exportsteuerdatei zum Filtern der Objekte im Modellrepository, die Sie exportieren möchten.

Wenn das zu exportierende Projekt Referenztabellen enthält, müssen Sie den Befehl über das Informatica-Dienste-Installationsverzeichnis ausführen. Der Befehl exportiert die Referenztabellenmetadaten aus dem Modellrepository in die XML-Datei. Der Befehl exportiert die Referenztabellendaten in eine ZIP-Datei. Wenn Sie den Befehl ausführen, geben Sie den Pfad und Dateinamen der zu erstellenden XML- und ZIP-Dateien an.

Der Befehl exportiert keine leeren Ordner.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, erhöhen Sie den verfügbaren Speicher für „infacmd“. Um den Systemspeicher zu erhöhen, legen Sie den Wert -Xmx in der Umgebungsvariable ICMD\_JAVA\_OPTS fest.

Der Befehl „infacmd tools exportObjects“ verwendet folgende Syntax:

```
exportObjects
<-DomainName|-dn> Domain name
<-UserName|-un> User name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> Security domain]
<-ProjectName|-pn> Project name
<-RepositoryService|-rs> Model Repository Service name
<-ExportFilePath|-fp> Path of file to export to
[<-OverwriteExportFile|-ow> Set to "true" to overwrite export file if it exists.]
[<-ControlFilePath|-cp> Path of export control file]
[<-OtherOptions|-oo>]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd tools exportObjects“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	Domänenname	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ProjectName -pn	Projektname	Erforderlich. Name des Projekts, aus dem die Objekte exportiert werden.
-RepositoryService -rs	Name des Modellrepository-Diensts	Erforderlich. Name des Modellrepository-Diensts.

Option	Argument	Beschreibung
-ExportFilePath -fp	Pfad der Datei zum Exportieren in	Erforderlich. Pfad und Name der XML-Datei der zu erstellenden Exportdatei. Sie können einen absoluten Pfad oder einen relativen Pfad zum Dateinamen angeben. Verwenden Sie einen einfach zu unterscheidenden Namen für die Datei. Verwenden Sie beispielsweise die folgende vorgeschlagene Namenskonvention:  <code>exp_&lt;project_name&gt;</code>  <b>Hinweis:</b> Der Befehl fügt die XML-Dateierweiterung an die Ausgabedatei an.
-OverwriteExportFile -ow	Setzen Sie die Option auf „true“, um gegebenenfalls eine Exportdatei zu überschreiben.	Optional. Legen Sie die Option auf TRUE fest, um eine vorhandene Exportdatei zu überschreiben. Wenn eine Exportdatei vorhanden und diese Option auf FALSE festgelegt ist, schlägt der Export fehl. Standardwert ist FALSE.
-ControlFilePath -cp	Pfad der Exportsteuerungsdatei	Optional. Pfad und Dateiname der Exportsteuerdatei, die die zu exportierenden Objekte filtert. Sie können einen absoluten Pfad oder einen relativen Pfad für den Dateinamen angeben.
-OtherOptions -oo	-	Erforderlich, wenn das zu exportierende Projekt Referenztabellen enthält. Zusätzliche Optionen zum Exportieren von Referenztabellendaten in eine ZIP-Datei. Geben Sie die Optionen in folgendem Format ein:  <code>rtm:&lt;option_name&gt;=&lt;value&gt;,&lt;option_name&gt;=&lt;value&gt;</code>  Zu den erforderlichen Optionsnamen gehören: <ul style="list-style-type: none"> <li>- <code>disName</code>. Name des Datenintegrationsdiensts.</li> <li>- <code>codePage</code>. Codepage der Referenzdaten.</li> <li>- <code>refDataFile</code>. Pfad und Dateiname der ZIP-Datei, in die Sie die Referenztabellendaten exportieren möchten.</li> </ul> <b>Beispiel:</b>  <code>rtm:disName=ds,codePage=UTF-8,refDataFile=/folder1/data.zip</code>

## exportResources

Exportiert die Scorecard-Objekte und Herkunftsinformationen in einem Projekt oder Ordner in eine XML-Datei, die Sie in Metadata Manager verwenden.

Wenn Sie nicht alle Objekte im Projekt exportieren möchten, verwenden Sie eine infacmd-Exportsteuerdatei zum Filtern der zu exportierenden Objekte. Der Befehl exportiert keine leeren Ordner.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, erhöhen Sie den verfügbaren Speicher für „infacmd“. Um den Systemspeicher zu erhöhen, legen Sie den Wert `-Xmx` in der Umgebungsvariable `ICMD_JAVA_OPTS` fest.



Der Befehl „infacmd tools exportResources“ verwendet folgende Syntax:

```
exportResources

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-ProjectName|-pn> project_name

<-RepositoryService|-rs> model_repository_service_name

<-ExportFilePath|-fp> export_file_path

[<-OverwriteExportFile|-ow> overwrite_export_file]

[<-ControlFilePath|-cp> control_file_path]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd tools exportResources“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ProjectName -pn	project_name	Erforderlich. Name des Projekts, aus dem die Objekte exportiert werden.
-RepositoryService -rs	model_repository_service_name	Erforderlich. Name des Modellrepository-Diensts.
-ExportFilePath -fp	export_file_path	<p>Erforderlich. Pfad und XML-Dateiname der Exportdatei, die beim Ausführen des Befehls vom Befehlszeilenprogramm erstellt wird. Sie können einen absoluten Pfad oder einen relativen Pfad für den Dateinamen angeben. Verwenden Sie einen eindeutigen Namen für die Datei. Verwenden Sie beispielsweise die folgende vorgeschlagene Namenskonvention:</p> <p>exp_&lt;project_name&gt;.xml</p>
-OverwriteExportFile -ow	overwrite_export_file	Optional. Legen Sie die Option auf „True“ fest, um eine vorhandene Exportdatei zu überschreiben. Wenn eine Exportdatei vorhanden ist und Sie diese Option auf „False“ festlegen, schlägt der Export fehl. Standardwert ist „False“.
-ControlFilePath -cp	control_file_path	Optional. Pfad und Dateiname der Exportsteuerdatei, die die vom Befehlszeilenprogramm exportierten Objekte filtert. Sie können einen absoluten Pfad oder einen relativen Pfad für den Dateinamen angeben.

## importObjects

Importiert Objekte aus einer XML-Datei in ein vorhandenes Projekt im Modellrepository.

Wenn Sie nicht alle Objekte in der Datei importieren möchten, verwenden Sie eine infacmd-Importsteuerdatei zum Filtern der Objekte im Modellrepository, die Sie importieren möchten.

Wenn die zu importierende Datei Referenztabelle enthält, müssen Sie den Befehl über das Informatica-Dienste-Installationsverzeichnis ausführen. Der Befehl importiert die Referenztabelle metadaten aus der XML-Datei in das Modellrepository. Der Befehl importiert die Referenztabelle metadaten aus einer ZIP-Datei.

Wenn Sie den Befehl ausführen, geben Sie den Pfad und Dateinamen der zu importierenden XML- und ZIP-Dateien an.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, erhöhen Sie den verfügbaren Speicher für „infacmd“. Um den Systemspeicher zu erhöhen, legen Sie den Wert „-Xmx“ in der Umgebungsvariable ICMD\_JAVA\_OPTS fest.

Der Befehl „infacmd tools importObjects“ verwendet folgende Syntax:

```
importObjects

<-DomainName|-dn> Domain name

<-UserName|-un> User name

<-Password|-pd> Password

[<-SecurityDomain|-sdn> Security domain]

[<-TargetProject|-tp> Target project name <ignored if control file is specified>]

<-RepositoryService|-rs> Model Repository Service name

<-ImportFilePath|-fp> import_file_path

[<-SourceProject|-sp> Source project name in import file <ignored if control file is
specified>]

[<-TargetFolder|-tf> Target folder to import to <omit for root, ignored if control file
is specified>]

[<-SkipCRC|-sc> Set to "true" to skip CRC check on imported file.]

[<-ConflictResolution|-cr> Resolution type]

[<-ControlFilePath|-cp> Path of import control file]

[<-SkipCnxValidation|-scv> Set to "true" to skip connection validation.]

[<-OtherOptions|-oo>]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd tools importObjects“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	Domänenname	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-TargetProject -tp	Zielprojektname <wird ignoriert, wenn Steuerungsdatei angegeben wurde>	Optional. Name des Projekts, in das die Objekte importiert werden sollen. Das Projekt muss im Repository vorhanden sein, bevor Sie die Objekte importieren. Die Option wird ignoriert, wenn Sie eine Importsteuerungsdatei verwenden.
-RepositoryService -rs	Name des Modellrepository-Diensts	Erforderlich. Name des Modellrepository-Diensts.
-ImportFilePath -fp	import_file_path	Erforderlich. Pfad und Dateiname der XML-Datei, aus der die Objekte importiert werden sollen. Sie können einen absoluten Pfad oder einen relativen Pfad für den Dateinamen angeben.
-SourceProject -sp	Name des Quellprojekts in Importdatei <wird ignoriert, wenn Steuerungsdatei angegeben wurde>	Optional. Name des Quellprojekts in der zu importierenden Datei. Die Option wird ignoriert, wenn Sie eine Importsteuerungsdatei verwenden.
-TargetFolder -tf	Zielordner zum Importieren in <für Root weglassen, wird ignoriert, wenn Steuerungsdatei angegeben wurde>	Optional. Zielordner, in den Sie die Objekte importieren möchten. Wenn Sie keinen Zielordner angeben, werden die Objekte in das Zielprojekt importiert. Der Ordner muss im Repository vorhanden sein, bevor Sie die Objekte importieren. Die Option wird ignoriert, wenn Sie eine Importsteuerungsdatei verwenden.
-SkipCRC -sc	Legen Sie diese Option auf TRUE fest, um die CRC-Prüfung für die importierte Datei zu überspringen.	Gibt an, ob die zyklische Redundanzprüfung (Cyclic Redundancy Check, CRC) übersprungen werden soll, mit der festgestellt wird, ob die zu importierende Datei geändert wurde. Legen Sie die Option auf TRUE fest, um die Prüfung zu überspringen. Standardwert ist „false“.
-ConflictResolution -cr	Angegebener Lösungstyp	Optional. Konfliktlösungsstrategie. Sie können eine der folgenden Optionen für alle zu importierenden Objekte angeben: <ul style="list-style-type: none"> <li>- umbenennen</li> <li>- ersetzen</li> <li>- erneut verwenden</li> <li>- keine</li> </ul> Die Option wird ignoriert, wenn Sie eine Importsteuerungsdatei verwenden. Wenn die Konfliktlösungsstrategie auf KEINE festgelegt ist und ein Konflikt auftritt, schlägt der Import fehl. Standardwert ist „Keine“.
-ControlFilePath -cp	Pfad der Importsteuerungsdatei	Optional. Pfad und Dateiname der Importsteuerungsdatei, die die zu importierenden Objekte filtert. Sie können einen absoluten Pfad oder einen relativen Pfad angeben.

Option	Argument	Beschreibung
-SkipCnxValidation -scv	Legen Sie die Option auf TRUE fest, um die Verbindungsvalidierung zu überspringen.	<p>Optional. Gibt an, ob die Validierung der Zielverbindung während des Imports übersprungen werden soll. Der Importprozess stellt standardmäßig sicher, dass die von den importierten Objekten verwendeten Verbindungen im Zielrepository vorhanden sind. Wenn die Verbindungen nicht vorhanden sind, schlägt der Import fehl.</p> <p>Um die Validierung der Zielverbindung zu überspringen und mit dem Import fortzufahren, legen Sie diese Option auf TRUE fest. Wenn die importierten Objekte Verbindungen verwenden, die im Zielrepository nicht vorhanden sind, importiert der Importprozess die Objekte mit einer nicht angegebenen Verbindung. Verwenden Sie das Developer Tool, um nach Abschluss des Importprozesses die richtige Verbindung auszuwählen.</p> <p>Standardwert ist „false“.</p> <p><b>Hinweis:</b> Wenn eine Import-Steuerdatei eine Quellverbindung angibt, die in der Datei, die Sie importieren, nicht vorhanden ist, schlägt der Importprozess unabhängig vom Wert dieser Option fehl. Um den Fehler zu korrigieren, stellen Sie sicher, dass das rebind-Element für die Verbindung in der Import-Steuerdatei Quellverbindungen enthält, die in der von Ihnen importierten Datei vorhanden sind.</p>
-OtherOptions -oo	-	<p>Erforderlich, wenn die Importdatei Referenztabellen enthält. Zusätzliche Optionen für den Import von Referenztabellendaten aus einer ZIP-Datei. Geben Sie die Optionen in folgendem Format ein:</p> <pre>rtm:&lt;option_name&gt;=&lt;value&gt;,&lt;option_name&gt;=&lt;value&gt;</pre> <p>Zu den erforderlichen Optionsnamen gehören:</p> <ul style="list-style-type: none"> <li>- disName. Name des Datenintegrationsdiensts.</li> <li>- codePage. Codepage der Referenzdaten.</li> <li>- refDataFile. Pfad und Dateiname der ZIP-Datei, aus der Sie die Referenztabellendaten importieren möchten.</li> </ul> <p>Beispiel:</p> <pre>rtm:disName=ds,codePage=UTF-8,refDataFile=/folder1/data.zip</pre>

## patchApplication

Stellt mithilfe einer .piar-Datei eine Anwendungs-Patch für einen Datenintegrationsdienst bereit. Der Datenintegrationsdienst wendet den Patch auf die entsprechende inkrementelle Anwendung an. Die

inkrementelle Anwendung muss auf demselben Datenintegrationsdienst bereitgestellt werden, auf dem der Patch bereitgestellt werden soll.

Wenn Sie den Patch basierend auf einer früheren Version der inkrementellen Anwendung erstellt haben, steht der Patch unter Umständen nicht zur Verfügung. Ein Patch ist nicht verfügbar, wenn seit der Erstellung des aktuell bereitzustellenden Patches die Anwendungsobjekte im Patch von anderen Anwendungs-Patches aktualisiert wurden. Sie können die Anwendung des Patches durch den Datenintegrationsdienst erzwingen, um fortzufahren.

Sie können auch wählen, ob Sie Statusinformationen beibehalten oder verwerfen möchten. Statusinformationen verweisen auf Zuordnungseigenschaften und die Eigenschaften von Laufzeitobjekten, wie z. B. Zuordnungsausgaben oder die Sequenzgeneratorumwandlung.

Weitere Informationen zu Statusinformationen finden Sie im Kapitel „Anwendungsbereitstellung“ im *Informatica Developer Tool-Handbuch*.

**Hinweis:** Wenn Sie eine frühere Version eines Patches bereitstellen, führt der Datenintegrationsdienst kein Rollback der inkrementellen Anwendung auf den Zeitpunkt der Patch-Erstellung durch. Der Datenintegrationsdienst aktualisiert die Anwendung auf Basis der Anwendungsobjekte im Patch.

Der Befehl „`infacmd tools patchApplication`“ verwendet folgende Syntax:

```
patchApplication  
  
<-DomainName|-dn> Domain name  
  
<-UserName|-un> User name  
  
<-Password|-pd> Password  
  
[<-SecurityDomain|-sdn> Security domain]  
  
<-DataIntegrationService|-dis> Data Integration Service name  
  
<-FilePath|-fp> Patch file path  
  
[<-force|-f> True | False]  
  
[<-RetainStateInformation|-rsi> True | False]
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd tools patchApplication`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	Domänenname	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariablen <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariablen <code>INFA_DEFAULT_SECURITY_DOMAIN</code> festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-DataIntegrationService -dis	Name des Datenintegrationsdiensts	Erforderlich. Der Name des Datenintegrationsdiensts, auf dem die inkrementelle Anwendung bereitgestellt wird.
-FilePath -fp	Pfad der Patch-Datei	Erforderlich. Pfad und Dateiname (.piar) des bereitzustellenden Patches. Sie können einen absoluten Pfad oder einen relativen Pfad für den Dateinamen angeben.
-force -f	True False	Optional. Verwenden Sie <code>true</code> , um die Gültigkeit des Patches zu ignorieren und den Datenintegrationsdienst zu zwingen, den Patch auf die Anwendung anzuwenden. Standardwert ist <code>false</code> .
-RetainStateInformation -rsi	True False	Optional. Gibt an, ob Statusinformationen beibehalten oder verworfen werden. <b>Hinweis:</b> Diese Option überschreibt die Einstellung zum Beibehalten oder Verwerfen von Statusinformationen in der Anwendungs-Patch-Archivdatei.



# KAPITEL 38

## infacmd wfs-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [abortWorkflow, 1237](#)
- [bulkComplete, 1239](#)
- [cancelWorkflow, 1241](#)
- [completeTask, 1243](#)
- [createTables, 1245](#)
- [delegateTask, 1247](#)
- [dropTables, 1249](#)
- [listActiveWorkflowInstances, 1251](#)
- [listMappingPersistedOutputs, 1253](#)
- [listTasks, 1255](#)
- [listWorkflowParams, 1258](#)
- [listWorkflows, 1261](#)
- [pruneOldInstances, 1263](#)
- [recoverWorkflow, 1265](#)
- [releaseTask, 1267](#)
- [setMappingPersistedOutputs, 1269](#)
- [startTask, 1272](#)
- [startWorkflow, 1273](#)
- [upgradeWorkflowParameterFile, 1276](#)

### abortWorkflow

Bricht eine laufende Arbeitsablaufinstanz ab.

Wenn eine Zuweisungsaufgabe oder ein exklusives Gateway ausgeführt wird, schließt der Datenintegrationsdienst die Aufgabe oder das Gateway ab. Nach Abbruch oder Abschluss der Aufgabe bricht der Dienst die Arbeitsablaufinstanz ab. Der Dienst beginnt nicht mit der Ausführung von nachfolgenden Arbeitsablaufobjekten.

Der Befehl „infacmd wfs abortWorkflow“ verwendet die folgende Syntax:

```
abortWorkflow

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

<-InstanceId|-iid> instance_id

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs abortWorkflow“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Arbeitsablaufinstanz ausführt.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-Instanceld -iid	Instanz-ID des abzubrechenden Arbeitsablaufs	Erforderlich. Abzubrechende Arbeitsablaufinstanz-ID. Sie können die Arbeitsablaufinstanz-ID in den Arbeitsablaufeigenschaften auf der Registerkarte „Überwachen“ des Administrator Tools lesen. Sie können aber auch „infacmd wfs listActiveWorkflowInstances“ ausführen, um nach der Arbeitsablaufinstanz-ID zu suchen.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## bulkComplete

Hält alle Vorgänge für eine Human-Aufgabe in einem bestimmten Arbeitsablauf an und übergibt die Datensätze, die von der Aufgabe angegeben werden, an die nächste Stufe im Arbeitsablauf. Der Befehl „bulkComplete“ aktualisiert den Status der Schritte in der Human-Aufgabe, um anzugeben, dass die Schritte abgeschlossen sind. Der von der Aufgabe ermittelte Status der Datensätze wird vom Befehl weder bearbeitet noch aktualisiert.

Der Befehl „bulkComplete“ verwendet die folgende Syntax:

```
bulkComplete

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

<-InstanceId|-iid> Instance_id

<-StepName|-sid> Step_name

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs bulkComplete“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Arbeitsablaufinstanz ausführt.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
Instanz-ID -iid	Instance_ID	Erforderlich. Eindeutiger Bezeichner für den Arbeitsablauf, der die abzuschließende Human-Aufgabe ausführt.  Sie können die Arbeitsablaufinstanz-ID in den Arbeitsablaufeigenschaften auf der Registerkarte „Überwachen“ des Administrator Tools lesen. Sie können aber auch „infacmd wfs listActiveWorkflowInstances“ ausführen, um nach der Arbeitsablaufinstanz-ID zu suchen.
StepName -sid	Step_name	Erforderlich. Der Name der Human-Task, die der Arbeitsablauf zum Erstellen der Human-Task-Instanzen verwendet.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## cancelWorkflow

Bricht eine laufende Arbeitsablaufinstanz ab. Wenn Sie eine Arbeitsablaufinstanz abbrechen, beendet der Datenintegrationsdienst die Verarbeitung aller laufenden Aufgaben sowie die Verarbeitung der Arbeitsablaufinstanz. Der Service beginnt nicht mit der Ausführung von nachfolgenden Objekten.

Der Befehl „infacmd wfs cancelWorkflow“ verwendet die folgende Syntax:

```
cancelWorkflow
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-InstanceID|-iid> instance_ID
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

Die folgende Tabelle beschreibt die Optionen und Argumente für „infacmd wfs cancelWorkflow“:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Arbeitsablaufinstanz ausführt.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-InstanceID -iid	instance_ID	Erforderlich. Abzubrechende Arbeitsablaufinstanz-ID. Sie können die Arbeitsablaufinstanz-ID in den Arbeitsablaufeigenschaften auf der Registerkarte „Überwachen“ des Administrator Tools lesen. Sie können aber auch „infacmd wfs listActiveWorkflowInstances“ ausführen, um nach der Arbeitsablaufinstanz-ID zu suchen.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## completeTask

Schließt eine von Ihnen angegebene Human-Task-Instanz ab.

Eine Human-Task-Instanz ist eine Gruppe von Datensätzen, die ein Arbeitsablauf einem Benutzer oder einer Gruppe für die Analyse in Informatica Analyst zuweist. Der Befehl „completeTask“ aktualisiert den Status der Aufgabeninstanz zu „Abgeschlossen“ und übergibt die Datensätze in der Aufgabeninstanz an einen anderen Schritt im Arbeitsablauf. Sie können den Befehl beispielsweise so konfigurieren, dass die Datensätze zur Überprüfung an eine andere Aufgabeninstanz gesendet werden.

Jede Human-Task-Instanz hat eine eindeutige Aufgabeninstanz-ID. Wenn Sie „infacmd wfs completeTask“ ausführen, geben Sie einen ID-Wert ein, um die abzuschließende Aufgabeninstanz zu identifizieren.

Sie können die Aufgabeninstanz-ID auf folgende Arten finden:

- Melden Sie sich bei Informatica Analyst an und zeigen Sie die Aufgabeninstanz-ID im Monitoring Tool an.
- Führen Sie „infacmd wfs listTasks“ aus.
- Fragen Sie den Unternehmensadministrator oder den Benutzer, der Eigentümer der Aufgabeninstanz ist. Der Unternehmensadministrator oder Benutzer kann die Aufgabeninstanz-ID in Informatica Analyst anzeigen.

Der Befehl „infacmd wfs completeTask“ verwendet die folgende Syntax:

```
completeTask
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
<-TaskId|-tid> task_id
<-NextTask|-to> next_task
```

[<-SecurityDomain|-sdn> security\_domain]

[<-ResilienceTimeout|-re> timeout\_period\_in\_seconds]

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs completeTask“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Arbeitsablaufinstanz ausführt.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-TaskID -tid	task_id	Erforderlich. Eindeutiger Bezeichner für die Human-Task-Instanz.
-NextTask -to	next_task	Erforderlich. Der Name des Schritts im Arbeitsablauf, an den der Befehl die Datensätze der Aufgabeninstanz übergibt.  Die Konfiguration der Human-Task im Arbeitsablauf bestimmt die Schritte, an die die Datensätze der Aufgabeninstanz übergeben werden können.



Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## createTables

Erstellt die Datenbanktabellen, in denen Laufzeitmetadaten für den Arbeitsablauf gespeichert werden. Der Befehl erstellt leere Tabellen. Geben Sie bei Ausführung des Befehls den Dienst an, der die Arbeitsabläufe ausführt.

Überprüfen Sie vor dem Erstellen der Datenbanktabellen die folgenden Optionen auf dem Datenintegrationsdienst, der die Arbeitsabläufe ausführt:

- Das Workflow Orchestration-Dienstmodul ist auf dem Datenintegrationsdienst aktiv.
- Mit den Eigenschaften des Workflow Orchestration-Diensts wird die Verbindung für die Datenbank angegeben, in der die Arbeitsablaufmetadaten gespeichert werden.

Der createTables-Befehl verwendet die folgende Syntax:

```
createTables
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs createTables“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts zum Ausführen der Arbeitsabläufe, die Metadaten in die Tabellen schreiben.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## delegateTask

Weist einem anderen Benutzer oder einer anderen Gruppe die Eigentümerschaft für eine Human-Task-Instanz zu.

Wenn die Aufgabeninstanz keinen Eigentümer hat, können Sie die Eigentümerschaft einem anderen Benutzer oder einer anderen Aufgabeninstanz zuweisen. Alternativ können Sie einem anderen Benutzer oder einer anderen Gruppe eine Aufgabeninstanz zuweisen, wenn der aktuelle Benutzer die Aufgabeninstanz nicht abschließen kann.

Sie können einem Benutzer oder einer Gruppe eine Aufgabeninstanz zuweisen, wenn Sie der Eigentümer der Aufgabeninstanz oder der Unternehmensadministrator für die Aufgabe sind. Außerdem können Sie die Aufgabeninstanz einem anderen Benutzer oder einer anderen Gruppe zuweisen, wenn Sie potenzieller Eigentümer der Aufgabeninstanz sind. Sie sind potenzieller Eigentümer, wenn Sie einer von mehreren Benutzern sind, denen die Aufgabeninstanz durch die Human-Task zugewiesen wurde, und kein Benutzer der Eigentümer der Aufgabe ist.

Wenn Sie „infacmd wfs delegateTask“ ausführen, geben Sie die Aufgabeninstanz-ID der zuzuweisenden Aufgabeninstanz ein.

Sie können die Aufgabeninstanz-ID auf folgende Arten finden:

- Melden Sie sich bei Informatica Analyst an und zeigen Sie die Aufgabeninstanz-ID im Monitoring Tool an.
- Führen Sie „infacmd wfs listTasks“ aus.
- Fragen Sie den Unternehmensadministrator oder den Benutzer, der Eigentümer der Aufgabeninstanz ist. Der Unternehmensadministrator oder Benutzer kann die Aufgabeninstanz-ID in Informatica Analyst anzeigen.

Der Befehl „infacmd wfs delegateTask“ verwendet die folgende Syntax:

```
delegateTask
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
<-TaskId|-tid> task_id
```

```

<-Entity|-to> to_entity

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs delegateTask“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Arbeitsablaufinstanz ausführt.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-TaskID -tid	task_id	Erforderlich. Bezeichner der zu delegierenden Human-Task-Instanz.
-Entity -to	to_entity	Erforderlich. Name des Benutzers oder der Gruppe in der Domäne, an den bzw. die der Befehl die Aufgabeninstanz delegieren muss.  Beispiel: Native\Mary.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## dropTables

Löscht die Datenbanktabellen, in denen Laufzeitmetadaten für den Arbeitsablauf gespeichert werden.

Der dropTables-Befehl verwendet die folgende Syntax:

```
dropTables
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs dropTables“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, der die Arbeitsabläufe ausführt, deren Daten gelöscht werden sollen.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## listActiveWorkflowInstances

Listet aktive Arbeitsablaufinstanzen auf. Eine aktive Arbeitsablaufinstanz ist eine Instanz, für die eine Aktion ausgeführt werden kann. Listet den Status, die Arbeitsablaufinstanz-ID, den Arbeitsablaufnamen und den Anwendungsnamen für jede aktive Arbeitsablaufinstanz auf.

Aktive Arbeitsablaufinstanzen umfassen laufende Arbeitsablaufinstanzen sowie für die Wiederherstellung aktivierte Arbeitsablaufinstanzen, die abgebrochen werden.

Der Befehl „infacmd wfs listActiveWorkflowInstances“ verwendet die folgende Syntax:

```
listActiveWorkflowInstances
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs listActiveWorkflowInstances“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Arbeitsablaufinstanzen ausführt.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>



# listMappingPersistedOutputs

Listet den Status aller dauerhaften Zuordnungsausgaben auf. Sie können die Werte der dauerhaften Zuordnungsausgabe mit dem `infacmd wfs setMappingPersistedOutputs`-Befehl aktualisieren.

Der `infacmd wfs listMappingPersistedOutputs`-Befehl verwendet die folgende Syntax:

```
listMappingPersistedOutputs
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-Workflow|-wf> workflow_name
<-MappingTaskInstance|-mti> mapping_task_instance_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd wfs listMappingPersistedOutputs`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts zum Ausführen des Arbeitsablaufs. Die Anwendung, die den Arbeitsablauf enthält, muss für einen Datenintegrationsdienst bereitgestellt werden.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomännennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung, die den Arbeitsablauf enthält.
-Workflow -wf	workflow_name	Erforderlich. Name des Arbeitsablaufs.
- mti	MappingTaskInstance	Erforderlich. Der Name einer Zuordnungsaufgabe, die die Zuordnungsausgaben erstellt hat.

# listTasks

Listet die Human-Task-Instanzen in der Arbeitsablauf-Datenbank auf, in denen Sie eine Rolle haben und die die von Ihnen angegebenen Filterkriterien erfüllen. Verwenden Sie die Befehlsoptionen, um einen oder mehrere Filter festzulegen.

Wenn Sie keine Filteroption festlegen, gibt der Befehl eine Liste der ersten 10 Human-Task-Instanzen in der Datenbank zurück, in denen Sie eine Rolle haben. Verwenden Sie die Option `-MaxTasks`, um die Anzahl der vom Befehl zurückgegebenen Task-Instanzen zu ändern.

In den folgenden Fällen haben Sie jeweils eine Rolle in einer Task-Instanz:

- Sie sind der aktuelle Besitzer der Task-Instanz.
- Sie sind potenzielle Besitzer einer Task-Instanz, die ein anderer Benutzer nicht besitzt. Sie sind z. B. Mitglied in einer Gruppe, deren Mitglieder den Besitz der Aufgabe beanspruchen können.
- Sie sind der Unternehmensadministrator für die Task-Instanz.

Die für den Befehl festgelegten Filteroptionen sind kumulativ. Wenn Sie mehrere Filteroptionen festlegen, gibt der Befehl eine Liste der Human-Task-Instanzen zurück, die alle von Ihnen festgelegten Optionen erfüllen.

Der Befehl wendet den Benutzernamen an, den Sie als Filter für die Task-Instanzen in der Arbeitsablauf-Datenbank übermitteln. Sie führen beispielsweise den Befehl `listTasks` mit dem Benutzernamen `Native\Mary` aus und legen die Option `-FilterByOwner` auf `Native\John` fest. Der Befehl gibt eine Liste der Task-Instanzen zurück, die John besitzt und für die Mary potenzielle Besitzerin oder Unternehmensadministratorin ist.

Der Befehl `infacmd wfs listTasks` verwendet die folgende Syntax:

```
listTasks

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-MaxTasks|-max> max_tasks]

[<-FilterByOwner|-ow> e.g. Native\user_name]

[<-FilterByStatus|-st> READY|RESERVED|IN_PROGRESS|SUSPENDED]

[<-FilterByCreationDate|-cd> e.g. 2024-12-31]

[<-FilterByType|-tt> CleanseTask|ClusterTask|CleanseTaskReviewTask|ClusterTaskReviewTask]

[<-FilterByDueDate|-dd> e.g. 2024-12-31]

[<-FilterByID|-tid> e.g. 42]

[<-FilterByName|-tn> e.g. "ExceptionStep {1 - 9}"]

[<-FilterByNameLike|-tnl> e.g. "Step {% - %}"]

[<-TasksOffset|-offset> tasks_offset]

[<-Role> role]

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs listTasks“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Arbeitsablaufinstanz ausführt.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-MaxTasks -max	max_tasks	Optional. Definiert eine Obergrenze für die Anzahl der Human-Task-Instanzen in der Liste, die der Befehl zurückgibt.  Standardmäßig gibt der Befehl „infacmd wfs listTasks“ eine Liste der ersten 10 Task-Instanzen zurück.  Sie können die Option -max in Verbindung mit der Option -offset verwenden.
-FilterByOwner -ow	z. B. Native\user_name	Optional. Filtert die Liste der Human-Task-Instanzen in der Arbeitsablauf-Datenbank nach dem Namen des Benutzers oder der Gruppe, die die Aufgabe besitzt.
-FilterByStatus -st	READY RESERVED  IN_PROGRESS SUSPENDED	Optional. Filtert die Liste der Human-Task-Instanzen in der Arbeitsablauf-Datenbank nach dem Aufgabenstatus.
-FilterByCreationDate -cd	z. B. 2024-12-31	Optional. Filtert die Liste der Human-Task-Instanzen in der Arbeitsablauf-Datenbank nach dem Erstellungsdatum der Aufgaben.
-FilterByType -tt	CleanseTask ClusterTask  CleanseTaskReviewTask  ClusterTaskReviewTask	Optional. Filtert die Liste der Human-Task-Instanzen in der Arbeitsablauf-Datenbank nach dem Aufgabentyp.

Option	Argument	Beschreibung
-FilterByDueDate -dd	z. B. 2024-12-31	Optional. Filtert die Liste der Human-Task-Instanzen in der Arbeitsablauf-Datenbank nach dem Abgabetermin der Aufgabe. Der Abgabetermin zeigt den aktuellen Stichtag für die Fertigstellung der Aufgabe an.
-FilterByID -tid	z. B. 42	Optional. Filtert die Liste der Human-Task-Instanzen in der Arbeitsablauf-Datenbank nach der ID der Human-Task-Instanz.
-FilterByName -tn	z. B. "ExceptionStep {1-9}"	Optional. Filtert die Liste der Human-Task-Instanzen in der Arbeitsablauf-Datenbank nach dem von Ihnen angegebenen Namen der Human-Task-Instanz. Verwenden Sie -FilterByName und -FilterByNameLike nicht in demselben Befehl.
-FilterByNameLike -tnl	z. B. "Schritt {% - %}"	Optional. Filtert die Liste der Human-Task-Instanzen in der Arbeitsablauf-Datenbank nach dem Namen der Human Task und lässt in Platzhalterzeichen in der Filterzeichenfolge zu. Sie können das Prozentzeichen (%) als Platzhalterzeichen verwenden. Verwenden Sie -FilterByName und -FilterByNameLike nicht in demselben Befehl.
-TasksOffset -offset	tasks_offset	Optional. Gibt einen Offset von der ersten Task-Instanz in der Liste der Task-Instanzen an, die die Filterkriterien erfüllen.  Wenn Sie einen Offset angeben, überspringt der Befehl die vom Offset angegebenen Task-Instanzen und gibt eine Liste zurück, die mit der nächsten Instanz beginnt, die die Filterkriterien erfüllt.  Sie können die Option -offset mit der Option -max verwenden, um die Ergebnisse aufeinander folgender listTasks-Befehle zu organisieren. Wenn Sie z. B. infacmd WFS listTasks mit einem Wert von 50 ausführen, geben Sie eine Liste der Task-Instanzen im Bereich 1 bis 50 zurück. Wenn Sie den Befehl mit einem -max-Wert von 50 und einem -offset-Wert von 51 ausführen, wird die Liste der Tasks im Bereich von 51 bis 100 zurückgegeben.
-Role	-role	Optional. Filtert die Liste der Human-Task-Instanzen in der Arbeitsablauf-Datenbank nach der Human-Task-Rolle.  Sie können die folgenden Werte eingeben: - ADMINISTRATORS - ALLE - OWNERS - POTENTIAL_OWNERS  Wenn Sie die Option nicht festlegen, gibt der Befehl Task-Instanzen für alle Rollen zurück.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## listWorkflowParams

Listet die Parameter für einen Arbeitsablauf auf und erstellt eine Parameterdatei, die Sie für die Ausführung eines Arbeitsablaufs verwenden können. Der Befehl gibt eine XML-Datei mit Standardwerten zurück, die Sie aktualisieren können. Geben Sie den Parameterdateinamen an, wenn Sie den Arbeitsablauf mit infacmd wfs startWorkflow ausführen.

Der Befehl „infacmd wfs listWorkflowParams“ verwendet die folgende Syntax:

```
listWorkflowParams
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-Workflow|-wf> workflow_name
[<-OutputFile|-o> output_file_to_write_to]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs listWorkflowParams“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts zum Ausführen des Arbeitsablaufs. Die Anwendung, die den Arbeitsablauf enthält, muss für einen Datenintegrationsdienst bereitgestellt werden.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung, die den Arbeitsablauf enthält.
-Workflow -wf	workflow_name	Erforderlich. Name des Arbeitsablaufs.
- OutputFile -o	output file_to_write_to	Optional. Pfad und Dateiname der zu erstellenden Parameterdatei. Wenn Sie keine Datei angeben, zeigt der Befehl die Parameter in der Eingabeaufforderung an.

## listWorkflowParams-Ausgabe

Der listWorkflowParams-Befehl gibt eine Parameterdatei als XML-Datei mit Standardwerten zurück, die Sie aktualisieren können.

Sie führen zum Beispiel den listWorkflowParams-Befehl in der Anwendung "MyApp" und im Arbeitsablauf "MyWorkflow" aus. Der Arbeitsablauf „MyWorkflow“ verfügt über einen Parameter mit der Bezeichnung „MyParameter“.

Der listWorkflowParams-Befehl gibt eine XML-Datei in folgendem Format zurück:

```
<?xml version="1.0" encoding="UTF-16LE"?>
<root xmlns="http://www.informatica.com/Parameterization/1.0"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema"
      version="2.0"><!--Specify deployed application specific parameters here.--><!--
  <application name="MyApp">
    <workflow name="MyWorkflow"/>
  </application>--><project name="MyProject">
    <workflow name="MyWorkflow">
      <parameter name="MyParameter">Default</parameter>
    </workflow>
  </project>
</root>
```

Die Ausgabe-XML-Datei hat die folgenden Elemente der obersten Ebene:

### Anwendungselement

Wenn Sie einen Parameter in einem Element auf der obersten Ebene der Anwendung definieren, wendet der Data Integration Service den Parameterwert an, wenn Sie den angegebenen Arbeitsablauf in der angegebenen Anwendung ausführen. Sie müssen mindestens ein Projektelement in eine Anwendung/ einen Arbeitsablauf einbeziehen.

Standardmäßig befindet sich dieses Element auf der obersten Ebene in den Kommentaren. Entfernen Sie die Kommentare (!-- and -->), um dieses Element zu verwenden.



## Projektelement

Wenn Sie einen Parameter in einem Element auf der obersten Ebene eines Projekts definieren, wendet der Data Integration Service den Parameterwert auf den angegebenen Arbeitsablauf in dem Projekt in allen bereitgestellten Anwendungen an. Der Dienst wendet den Parameterwert auch auf alle Arbeitsabläufe an, die die Objekte im Projekt verwenden.

Wenn Sie in einem Projekt denselben Parameter in einem Element auf der obersten Ebene einer Anwendung und ein Element in derselben Parameterdatei definieren, hat der im Anwendungselement definierte Parameterwert Vorrang.

# listWorkflows

Listet die Arbeitsabläufe in einer Anwendung auf.

Der Befehl „`infacmd wfs listWorkflows`“ verwendet die folgende Syntax:

```
listWorkflows
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd wfs listWorkflows`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts zum Ausführen der Arbeitsabläufe. Die Anwendung, die die Arbeitsabläufe enthält, muss für einen Datenintegrationsdienst bereitgestellt werden.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	Passwort	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-Application -a	application_name	<p>Erforderlich. Name der Anwendung, die die Arbeitsabläufe enthält.</p>

# pruneOldInstances

Löscht Arbeitsablaufprozessdaten aus der Arbeitsablaufdatenbank.

Wenn der Datenintegrationsdienst einen Arbeitsablauf ausführt, schreibt der Arbeitsablaufprozess Daten in die Arbeitsablaufdatenbank. Im Laufe der Zeit kann sich die große Menge an Prozessdaten in der Datenbank negativ auf die Startgeschwindigkeit von Arbeitsablaufprozessen auswirken. Um Prozessdaten aus der Datenbank zu löschen, führen Sie den Befehl „wfs pruneOldInstances“ aus. Sie können den Befehl so konfigurieren, dass alle Prozessdaten in der Arbeitsablaufdatenbank gelöscht werden. Sie können auch nur jene Prozessdaten löschen, die in einem angegebenen Zeitraum generiert wurden.

Der Befehl „pruneOldInstances“ löscht nur Prozessdaten. Er löscht keine Daten, die von einer Arbeitsablaufinstanz oder einem Objekt im Arbeitsablauf gelesen oder geschrieben werden. Ebenso löscht der Befehl keine Metadaten von Arbeitsablaufobjekten.

Um die Prozessdaten zu löschen, müssen Sie in der Domäne über eine Dienstverwaltungsberechtigung verfügen.

Der Befehl „infacmd wfs pruneOldInstances“ verwendet die folgende Syntax:

```
pruneOldInstances
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-Days|-d> days
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für infacmd wfs pruneOldInstances beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Arbeitsablaufinstanz ausführt.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	password	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>

Option	Argument	Beschreibung
-Days -d	Tage	Der Zeitraum, dessen Prozessdaten gelöscht werden. Um den Zeitraum zu berechnen, wird die Anzahl der Tage, die Sie angeben, vom Datum und der Uhrzeit der Befehlsausführung abgezogen. Der Befehl löscht alle Prozessdaten, die die Arbeitsablaufprozesse in diesem Zeitraum generiert haben.  Geben Sie einen Wert zwischen 0 und 24855 ein. Wenn Sie 0 eingeben, löscht der Befehl alle Prozessdaten in der Arbeitsablaufdatenbank.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

## recoverWorkflow

Stellt eine Arbeitsablaufinstanz wieder her. Sie können eine Arbeitsablaufinstanz wiederherstellen, die von Ihnen abgebrochen oder durch einen behebbaren Fehler unterbrochen wurde. Wenn Sie eine Arbeitsablaufinstanz wiederherstellen, startet der Datenintegrationsdienst die Arbeitsablaufinstanz an der unterbrochenen Aufgabe neu und führt die unterbrochene Aufgabe erneut aus.

Der Befehl „infacmd wfs recoverWorkflow“ verwendet die folgende Syntax:

```
recoverWorkflow
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
<-InstanceID|-iid> instance_ID
[<-Wait|-w> true|false]
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

Die folgende Tabelle beschreibt die Optionen und Argumente für „infacmd wfs recoverWorkflow“:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die ursprüngliche Arbeitsablaufinstanz ausgeführt hat.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-InstanceID -iid	Instanz-ID des wiederherzustellenden Arbeitsablaufs	Erforderlich. Wiederherzustellende Arbeitsablaufinstanz-ID.  Sie können die Arbeitsablaufinstanz-ID in den Arbeitsablaufeigenschaften auf der Registerkarte „Überwachen“ des Administrator Tools lesen. Sie können aber auch „infacmd wfs listActiveWorkflowInstances“ ausführen, um nach der Arbeitsablaufinstanz-ID zu suchen.
-Wait -w	true false	Optional. Gibt an, ob infacmd bis zur Wiederherstellung der Arbeitsablaufinstanz wartet, bevor eine Rückkehr zur Shell oder Eingabeaufforderung erfolgt. Wenn TRUE, kehrt infacmd nach Wiederherstellung der Arbeitsablaufinstanz zur Shell oder Eingabeaufforderung zurück. Sie können nachfolgende Befehle erst ausführen, wenn die Arbeitsablaufinstanz wiederhergestellt wurde. Ist die Option auf FALSE festgelegt, kehrt infacmd sofort zur Shell oder Eingabeaufforderung zurück. Sie müssen nicht auf die Wiederherstellung der Arbeitsablaufinstanz warten, bis Sie den nächsten Befehl ausführen. Standardwert ist „false“.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## releaseTask

Gibt eine Human-Task-Instanz des aktuellen Eigentümers frei. Sie können eine Aufgabeninstanz freigeben, wenn Sie der Eigentümer oder der Unternehmensadministrator für die Aufgabeninstanz sind.

Wenn Sie eine Aufgabeninstanz freigeben, hat sie keinen Eigentümer mehr. Falls Sie eine Aufgabeninstanz freigeben, deren Eigentümer Sie sind, bleibt sie im Analyst Tool für Sie verfügbar. Wenn die Human-Task mehrere Benutzer als potenzielle Eigentümer der von Ihnen freigegebenen Aufgabeninstanz identifiziert, ist die Aufgabeninstanz für alle potenziellen Eigentümer verfügbar.

Der Befehl „infacmd wfs releaseTask“ verwendet die folgende Syntax:

```
releaseTask

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

<-TaskId|-tid> task_id

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs releaseTask“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Arbeitsablaufinstanz ausführt.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-TaskID -tid	task_id	Erforderlich. Bezeichner der Human-Task-Instanz in der Arbeitsablauf-Datenbank.



Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## setMappingPersistedOutputs

Aktualisiert die dauerhaften Zuordnungsausgaben für eine Zuordnungsaufgabeninstanz in einem Arbeitsablauf. Oder setzt die dauerhaften Zuordnungsausgaben auf Nullwerte. Mit den Befehlsoptionen werden der Instanzname der Zuordnungsaufgabe sowie der Name der Anwendung und des Arbeitsablaufs angegeben.

Geben Sie zum Aktualisieren eines Werts ein Namen-Wert-Paar ein, das den Namen der Zuordnungsausgabe und den Wert enthält, in den er geändert werden soll. Verwenden Sie zum Zurücksetzen eines dauerhaften Werts auf Nullwerte die Option zum Zurücksetzen. Sie können bestimmte oder alle Zuordnungsausgaben für eine Zuordnungsaufgabeninstanz zurücksetzen. Verwenden Sie zum Anzeigen dauerhafter Zuordnungsausgaben den infacmd listMappingPersistedOutputs-Befehl.

Der infacmd wfs setMappingPersistedOutputs-Befehl verwendet die folgende Syntax:

```
setMappingPersistedOutputs
<-DomainName|-dn> domain_name
[<-ServiceName|-sn> service_name]
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
```

```

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application_name

<-Workflow|-wf> workflow_name

<-MappingTaskInstance|-mti> mapping_task_instance_name]

<-outputValues|-onvp> space_separated_output_value_pairs

[<-resetOutputs |-reset> reset_outputs]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs setMappingPersistedOutputs“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts zum Ausführen des Arbeitsablaufs. Die Anwendung, die den Arbeitsablauf enthält, muss für einen Datenintegrationsdienst bereitgestellt werden.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung, die den Arbeitsablauf enthält.
-Workflow -wf	workflow_name	Erforderlich. Name des Arbeitsablaufs.
-MappingTaskInstance -mti	mappingTaskInstancenamen	Erforderlich. Der Name einer Zuordnungsaufgabe, die die Zuordnungsausgaben erstellt hat.
-outputvalues -onvp	space_separated_output_value_pairs	Optional. Ändert den dauerhaften Wert bestimmter Zuordnungsausgaben. Geben Sie durch Leerzeichen getrennte Namen-Wert-Paare in der folgenden Syntax ein: output_name=value output2_name=value output3_name=value
-ResetOutputs -reset	reset_outputs	Optional. Entfernt den Wert der Zuordnungsausgabe aus dem Repository. Geben Sie zum Zurücksetzen bestimmter Zuordnungsausgaben die Option zum Zurücksetzen mit durch Leerzeichen getrennten Zuordnungsausgabennamen in die folgende Syntax ein: -reset mapping_output_name mapping_output2_name mapping_output3_name

# startTask

Startet eine Human-Task-Instanz in einem Arbeitsablauf. Der Start-Vorgang ändert den Status der Aufgabeninstanz in IN\_PROGRESS.

Der Befehl „infacmd wfs startTask“ verwendet die folgende Syntax:

```
startTask  
  
<-DomainName|-dn> domain_name  
  
<-ServiceName|-sn> service_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
<-TaskId|-tid> task_id  
  
[<-SecurityDomain|-sdn> security_domain]  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs startTask“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Arbeitsablaufinstanz ausführt.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-TaskID -tid	task_id	Erforderlich. Bezeichner der zu startenden Human Task.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>

## startWorkflow

Startet eine Instanz eines Arbeitsablaufs. Sie können mehrere Instanzen eines Arbeitsablaufs gleichzeitig ausführen. Sie können eine Parameterdatei für den Arbeitsablauf oder einen Parametersatz verwenden.

Der Befehl „infacmd wfs startWorkflow“ verwendet die folgende Syntax:

```
startWorkflow
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-Workflow|-wf> workflow_name
[<-Wait|-w> true|false]
[<-ParameterFile|-pf> parameter_file_path]
```

```
[<-ParameterSet|-ps> parameter_set_name]
```

```
[<-OperatingSystemProfile|-osp> operating_system_profile_name]
```

Der Befehl gibt die Ablaufinstanz-ID aus.

Die folgende Tabelle beschreibt infacmd wfs startWorkflow-Optionen und -Argumente:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts zum Ausführen des Arbeitsablaufs. Die Anwendung, die den Arbeitsablauf enthält, muss für einen Datenintegrationsdienst bereitgestellt werden.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-Application -a	application_name	Erforderlich. Name der Anwendung, die den Arbeitsablauf enthält.
-Workflow -wf	workflow_name	Erforderlich. Name des zu startenden Arbeitsablaufs.
-Wait -w	true false	<p>Optional. Gibt an, ob infacmd bis zum Abschluss der Arbeitsablaufinstanz wartet, bevor eine Rückkehr zur Shell oder Eingabeaufforderung erfolgt. Wenn TRUE, kehrt infacmd nach Abschluss der Arbeitsablaufinstanz zur Shell oder Eingabeaufforderung zurück. Sie können nachfolgende Befehle erst ausführen, wenn die Arbeitsablaufinstanz abgeschlossen ist. Ist die Option auf FALSE festgelegt, kehrt infacmd sofort zur Shell oder Eingabeaufforderung zurück. Sie müssen nicht auf den Abschluss der Arbeitsablaufinstanz warten, bis Sie den nächsten Befehl ausführen. Standardwert ist „False“.</p>
-ParameterFile -pf	parameter_file_path	<p>Optional. Name und Pfad der Parameterdatei. Geben Sie einen Parameterdatei- und Parametersatznamen nicht im selben Befehl ein.</p>

Option	Argument	Beschreibung
-ParameterSet -ps	parameter_set_name	Optional. Name des zur Laufzeit zu verwendenden Parametersatzes. Die Parametersatzoption überschreibt alle mit einer Anwendung bereitgestellten Parametersätze.  Geben Sie einen Parameterdatei- und Parametersatznamen nicht im selben Befehl ein.
-OperatingSystemProfile -osp	operating_system_profile_name	Optional. Name des Betriebssystemprofils, unter dem der Arbeitsablauf ausgeführt wird.

## upgradeWorkflowParameterFile

Aktualisiert eine Arbeitsablaufparameterdatei, damit das Dateiformat mit der aktuellen Version kompatibel ist. Führen Sie den Befehl auf Arbeitsablaufparameterdateien aus, die Benutzer in einer Informatica 9.x-Version erstellt haben. Wenn Sie den Befehl ausführen, identifizieren Sie eine Arbeitsablaufparameterdatei für das Upgrade und geben eine Zielfeile an.

Der Befehl „`infacmd wfs upgradeWorkflowParameterFile`“ verwendet die folgende Syntax:

```

upgradeWorkflowParameterFile
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-Workflow|-wf> workflow_name
<-ParameterFile|-pf> parameter file path
<-TargetOutputFile|-of> output_file_path

```



In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs upgradeWorkflowParameterFile“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts zum Ausführen des Arbeitsablaufs. Die Anwendung, die den Arbeitsablauf enthält, muss für einen Datenintegrationsdienst bereitgestellt werden.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung, die den Arbeitsablauf enthält.
-Workflow -wf	workflow_name	Erforderlich. Name des Arbeitsablaufs, der die Parameterdatei mit den Werten liest.
-Wait -w	true false	Optional. Gibt an, ob infacmd bis zum Abschluss der Arbeitsablaufinstanz wartet, bevor eine Rückkehr zur Shell oder Eingabeaufforderung erfolgt. Wenn TRUE, kehrt infacmd nach Abschluss der Arbeitsablaufinstanz zur Shell oder Eingabeaufforderung zurück. Sie können nachfolgende Befehle erst ausführen, wenn die Arbeitsablaufinstanz abgeschlossen ist. Ist die Option auf FALSE festgelegt, kehrt infacmd sofort zur Shell oder Eingabeaufforderung zurück. Sie müssen nicht auf den Abschluss der Arbeitsablaufinstanz warten, bis Sie den nächsten Befehl ausführen. Standardwert ist „False“.
-ParameterFile -pf	parameter file path	Erforderlich. Name und Speicherort der Parameterdatei, die die zu aktualisierenden Werte enthält.
-TargetOutputFile -of	parameter file path	Erforderlich. Name und Speicherort der Ausgabedatei aus dem Befehl. Die Ausgabedatei enthält die gültigen Parameter für die aktuelle Version.

# KAPITEL 39

## infacmd ws-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [ListOperationOptions, 1279](#)
- [ListOperationPermissions, 1281](#)
- [ListWebServiceOptions, 1283](#)
- [ListWebServicePermissions, 1285](#)
- [ListWebServices, 1287](#)
- [RenameWebService, 1289](#)
- [SetOperationPermissions, 1291](#)
- [SetWebServicePermissions, 1294](#)
- [StartWebService, 1297](#)
- [StopWebService, 1299](#)
- [UpdateOperationOptions, 1300](#)
- [UpdateWebServiceOptions, 1303](#)

### ListOperationOptions

Listet die Eigenschaften eines Webdienstvorgangs auf, der in einem Datenintegrationsdienst bereitgestellt wird.

Der Befehl „infacmd ws ListOperationOptions“ verwendet die folgende Syntax:

```
ListOperationOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-WebService|-ws> web_service
<-Operation|-op> operation
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws ListOperationOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem der Webdienst bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-WebService -ws	web_service	Erforderlich. Name des Webediensts.
Operation -op	operation	Erforderlich. Name des Webedienstvorgangs, für den Eigenschaften aufgelistet werden sollen.

## ListOperationPermissions

Listet Gruppen- und Benutzerberechtigungen für eine Webserviceoperation auf. Sie müssen direkte oder effektive Berechtigungen angeben.

Der Befehl „`infacmd ws ListOperationPermissions`“ verwendet die folgende Syntax:

```
ListOperationPermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-WebService|-ws> web_service
<-Operation|-op> operation
<<-Direct> direct_permission_only|<-Effective> effective_permission_only
```

In der folgenden Tabelle werden die Optionen und Argumente für „`infacmd ws ListOperationPermissions`“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable <code>INFA_DEFAULT_DOMAIN</code> festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem der Webedienst bereitgestellt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	Passwort	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänenennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-WebService -ws	web_service	Erforderlich. Name des Webdiensts.
-Operation -op	operation	Erforderlich. Name des Webdienstvorgangs, für den Eigenschaften aufgelistet werden sollen.
-Direct oder -Effective	direct_permission_only effective_permission_only	Erforderlich. Geben Sie Direct ein, um zugewiesene Berechtigungen aufzulisten. Geben Sie Effective ein, um geerbte Berechtigungen aufzulisten.

## ListWebServiceOptions

Listen Sie die Eigenschaften eines Webdiensts auf, der in einem Datenintegrationsdienst bereitgestellt wird. Sie können die Eigenschaften unter Verwendung des Administrator-Tools oder infacmd ws UpdateWebServiceOptions konfigurieren.

Der Befehl „infacmd ws ListWebServiceOptions“ verwendet die folgende Syntax:

```
ListWebServiceOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-WebService|-ws> web_service
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws ListWebServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem der Webdienst bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.



Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-WebService -ws	web_service	Erforderlich. Name des Webservice.

## ListWebServicePermissions

Listet Gruppen- und Benutzerberechtigungen für einen Webservice auf, der in einem Datenintegrationsdienst bereitgestellt wird. Sie müssen direkte oder effektive Berechtigungen angeben.

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws ListWebServicePermissions“ beschrieben:

```
ListWebServicePermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-WebService|-ws> web_service
<<-Direct> direct_permission_only|<-Effective> effective_permission_only
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws ListWebServicePermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domännennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domännennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem der Webdienst bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-WebService -ws	web_service	Erforderlich. Name des Webdiensts.
-Direct oder -Effective	direct_permission_only effective_permission_only	Erforderlich. Geben Sie Direct ein, um zugewiesene Berechtigungen aufzulisten. Geben Sie Effective ein, um geerbte Berechtigungen aufzulisten.

## ListWebServices

Listet die Webdienste für eine Anwendung auf. Wenn Sie keinen Anwendungsnamen eingeben, listet infacmd alle Webdienste für einen Datenintegrationsdienst auf.

Der Befehl „infacmd ws ListWebServices“ verwendet die folgende Syntax:

```
ListWebServices
<-DomainName|-dn> domain_name
```

```

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-WebService|-ws> web_service

[<-Application|-a> application]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws ListWebServices“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Webdienste bereitgestellt werden.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-application -ap	anwendung	<p>Optional. Name der Anwendung, für die Webdienste aufgelistet werden sollen.</p>

## RenameWebService

Umbenennen eines Webdiensts.

Der Befehl „infacmd ws RenameWebService“ verwendet die folgende Syntax:

```

RenameWebService
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-WebService|-ws> web_service
<-NewName|-n> new_name

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws RenameWebService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem der Webdienst bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-WebService -ws	web_service	Erforderlich. Name des Webdiensts.
-NewName -n	new_name	Erforderlich. Neuer Name für den Webdienst.

## SetOperationPermissions

Legt die Gruppen- und Benutzerberechtigungen für einen Webdienstvorgang fest. Sie können Berechtigungen für einen Benutzer oder eine Gruppe festlegen oder verweigern.

Der Befehl „`infacmd ws SetOperationPermissions`“ verwendet die folgende Syntax:

```
SetOperationPermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-WebService|-ws> web_service
<-Operation|-op> operation
<-GranteeUserName|-gun> grantee_user_name|
<-GranteeGroupName|-ggn> grantee_group_name>
[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]
[<-AllowedPermissions|-ap> list_of_allowed_permissions_separated_by_space]
[<-DeniedPermissions|-dp> list_of_denied_permissions_separated_by_space]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws SetOperationPermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem der Webdienst bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.



Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-WebService -ws	web_service	Erforderlich. Name des Webdiensts.
-Operation -op	Operation	Erforderlich. Name des Webdienstvorgangs.
-GranteeUserName GranteeGroupName -gun ggn	grantee_user_name  grantee_group_name	Erforderlich. Benutzername bzw. Gruppenname, für den Berechtigungen festgelegt oder verweigert werden sollen.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, der der Benutzer angehört.

Option	Argument	Beschreibung
-AllowedPermissions -ap	list_of_allowed_permissions_separated_by_space	Erforderlich. Liste der zulässigen Berechtigungen. Geben Sie einen der folgenden Parameter durch Leerzeichen getrennt ein: <ul style="list-style-type: none"> <li>- GRANT. Benutzer können mithilfe des Administrator-Tools oder des infacmd-Befehlszeilenprogramms Berechtigungen für die Operation gewähren oder widerrufen.</li> <li>- EXECUTE. Benutzer können die Operation ausführen.</li> </ul>
-DeniedPermissions -dp	list_of_denied_permissions_separated_by_space	Optional. Liste der Berechtigungen, die Benutzern verweigert werden sollen. Geben Sie einen der folgenden Parameter durch Leerzeichen getrennt ein: <ul style="list-style-type: none"> <li>- GRANT. Benutzer können Berechtigungen für den Vorgang weder gewähren noch entziehen.</li> <li>- EXECUTE. Benutzer können den Vorgang nicht ausführen.</li> </ul>

## SetWebServicePermissions

Legt die Benutzer- oder Gruppenberechtigungen für einen Webdienst fest. Sie können Berechtigungen für einen Benutzer oder eine Gruppe festlegen oder verweigern.

Der Befehl „infacmd ws SetWebServicePermissions“ verwendet die folgende Syntax:

```
SetWebServicePermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-WebService|-ws> web_service
<-GranteeUserName|-gun> grantee_user_name|
<-GranteeGroupName|-ggn> grantee_group_name>
[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]
[<-AllowedPermissions|-ap> list_of_allowed_permissions_separated_by_space]
[<-DeniedPermissions|-dp> list_of_denied_permissions_separated_by_space]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws SetWebServicePermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem der Webdienst bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-WebService -ws	web_service	Erforderlich. Name des Webdiensts.
-GranteeUserName GranteeGroupName -gun -ggn	grantee_user_name  grantee_group_name	Erforderlich. Benutzername bzw. Gruppenname, für den Berechtigungen festgelegt oder verweigert werden sollen.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, der der Benutzer angehört.

Option	Argument	Beschreibung
-AllowedPermissions -ap	list_of_allowed_permissions_separated_by_space	Erforderlich. Liste der zulässigen Berechtigungen. Geben Sie einen der folgenden Parameter durch Leerzeichen getrennt ein: <ul style="list-style-type: none"> <li>- GRANT. Benutzer können mithilfe des Administrator-Tools oder des infacmd-Befehlszeilenprogramms Berechtigungen für den Webdienst gewähren oder widerrufen.</li> <li>- EXECUTE. Benutzer können den Webdienst ausführen.</li> </ul>
-DeniedPermissions -dp	list_of_denied_permissions_separated_by_space	Optional. Liste der Berechtigungen, die Benutzern verweigert werden sollen. Geben Sie einen der folgenden Parameter durch Leerzeichen getrennt ein: <ul style="list-style-type: none"> <li>- GRANT. Benutzer können Berechtigungen für den Webdienst weder gewähren noch entziehen.</li> <li>- EXECUTE. Benutzer können den Webdienst nicht ausführen.</li> </ul>

## StartWebService

Startet einen Webdienst, der in einem Datenintegrationsdienst bereitgestellt wird.

Der Befehl „infacmd ws StartWebService“ verwendet die folgende Syntax:

```
StartWebService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-WebService|-ws> web_service
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws StartWebService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Name des Datenintegrationsdiensts, in dem der Webdienst bereitgestellt wird.
-WebService -ws	web_service	Erforderlich. Name des zu startenden Webdiensts.

## StopWebService

Stoppt einen laufenden Webdienst.

Der Befehl „infacmd ws StopWebService“ verwendet die folgende Syntax:

```
StopWebService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-WebService|-ws> web_service
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws StopWebService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Name des Datenintegrationsdiensts, in dem der Webdienst bereitgestellt wird.
-WebService -ws	web_service	Erforderlich. Name des zu beendenden Webdiensts.

## UpdateOperationOptions

Aktualisiert die Eigenschaften einer Webdienst-Operation, die in einem Datenintegrationsdienst bereitgestellt wird.

Der Befehl „infacmd ws UpdateOperationOptions“ verwendet die folgende Syntax:

```
UpdateOperationOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
```



```

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-WebService|-ws> web_service

<-Operation|-op> operation

<-Options|-o> options

```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws UpdateOperationOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem der Webdienst bereitgestellt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie den Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-WebService -ws	web_service	Erforderlich. Name des Webdiensts.
Operation -op	operation	Erforderlich. Name des zu aktualisierenden Webdienstvorgangs.
-Options -o> options	optionen	<p>Geben Sie die Webdienstoption im folgenden Format ein:</p> <pre>... -o option_type.option_name=value</pre>

## Operationsoptionen

Verwenden Sie Operationsoptionen zum Aktualisieren einer Web-Dienst-Operation. Verwenden Sie die Operationsoptionen mit infacmd ws UpdateOperationOptions.

Geben Sie Operationsoptionen in folgendem Format ein:

```
... -o OperationOptions.option_name=value ...
```

In der folgenden Tabelle wird eine Option für infacmd ws UpdateOperationOptions beschrieben:

Option	Beschreibung
WebServiceOperationOptions.ResultSetCacheExpirationPeriod	Zeitraum in Millisekunden, während dem der Ergebnissatz-Cache verwendet werden kann. Wenn der Wert auf -1 festgelegt ist, läuft der Cache nie ab. Wenn der Wert auf 0 festgelegt ist, ist das Ergebnissatz-Caching deaktiviert. Wenn alle Caches denselben Ablaufzeitraum verwenden sollen, bereinigen Sie den Ergebnissatz-Cache, nachdem Sie den Ablaufzeitraum geändert haben. Default is 0.

## UpdateWebServiceOptions

Aktualisiert die Eigenschaften für einen Webdienst, der in einem Datenintegrationsdienst bereitgestellt wird. Um die Eigenschaften für diesen Webdienst anzuzeigen, können Sie infacmd ws ListWebServiceOptions verwenden.

Der Befehl „infacmd ws UpdateWebServiceOptions“ verwendet die folgende Syntax:

```
UpdateWebServiceOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-WebService|-ws> web_service
<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws UpdateWebServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem der Webdienst bereitgestellt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-Password -pd	Passwort	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-SecurityDomain -sdn	security_domain	<p>Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.</p>
-WebService -ws	web_service	Erforderlich. Name des Webdiensts.
-Options -o> options	optionen	Geben Sie jede Option durch ein Leerzeichen getrennt ein.

## Web-Dienst-Optionen

Verwenden Sie eine bestimmte Syntax für die Eingabe von Web-Dienst-Optionen.

Geben Sie Web-Dienst-Optionen im folgenden Format ein:

```
... -o option_type.option_name=value
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden Web-Dienst-Optionen beschrieben:

Option	Beschreibung
WebServiceOptions.startupType	Legt fest, ob der Web-Dienst zur Ausführung aktiviert ist, wenn die Anwendung startet oder wenn Sie den Web-Dienst starten. Geben Sie "enabled" oder "disabled" ein.
WebServiceOptions.traceLevel	Level der in das Web-Dienst-Protokoll zur Laufzeit geschriebenen Fehlermeldungen. Geben Sie eine der folgenden Meldungslevel ein: <ul style="list-style-type: none"><li>- AUS</li><li>- SCHWERWIEGEND</li><li>- WARNUNG</li><li>- INFO</li><li>- FEIN</li><li>- SUPERFEIN</li><li>- ALLE</li></ul>
WebServiceOptions.requestTimeout	Maximale Anzahl an Millisekunden, in denen der Data Integration Service ein Operations-Mapping ausführt, bevor die Web-Dienst-Anfrage abläuft. Standardwert ist 3.600.000.
WebServiceOptions.maxConcurrentRequests	Maximale Anzahl an Anfragen, die der Web-Dienst auf einmal verarbeiten kann. Standardwert ist 10.
WebServiceOptions.sortOrder	Sortierreihenfolge, die der Data Integration Service zum Sortieren und Vergleichen von Daten verwendet, wenn er im Unicode-Modus ausgeführt wird. Die Standardeinstellung ist "binär".
WebServiceOptions.EnableTransportLayerSecurity	Gibt an, dass der Web-Dienst HTTPS verwenden muss. Wenn der Data Integration Service nicht zur Verwendung von HTTPS konfiguriert ist, wird der Web-Dienst nicht gestartet. Geben Sie TRUE oder FALSE ein.
WebServiceOptions.EnableWSSecurity	Aktiviert den Data Integration Service zu Validierung der Benutzeranmeldedaten sowie zur Sicherstellung, dass der Benutzer zur Ausführung der Web-Dienst-Operationen berechtigt ist. Geben Sie TRUE oder FALSE ein.

Option	Beschreibung
WebServiceOptions.optimizeLevel	<p>Die Optimierungsebene, die der Data Integration Service für das Objekt anwendet. Geben Sie den numerischen Wert ein, der mit der Optimierungsebene verbunden ist, die Sie konfigurieren möchten. Sie können Sie einen der folgenden numerischen Werte eingeben:</p> <ul style="list-style-type: none"> <li>- 0. Der Datenintegrationsdienst wendet keine Optimierung an.</li> <li>- 1. Der Datenintegrationsdienst wendet die frühe Projektionsoptimierungsmethode an.</li> <li>- 2. Der Datenintegrationsdienst wendet die Optimierungsmethoden „Frühe Projektion“, „Frühe Auswahl“, „Push-Into“ und „Prädikat“ an.</li> <li>- 3. Der Datenintegrationsdienst wendet die Optimierungsmethoden „Kostenbasiert“, „Frühe Projektion“, „Frühe Auswahl“, „Push-Into“, „Prädikat“ und „Semi-Join“ an.</li> </ul>
WebServiceOptions.DTMKeepAliveTime	<p>Anzahl der Millisekunden, für die die DTM-Instanz geöffnet bleibt, nachdem sie die letzte Anfrage abgeschlossen hat. Webdienstanfragen für denselben Vorgang können die offene Instanz wiederverwenden. Verwenden Sie die Keep Alive-Zeit, um die Leistung zu erhöhen, wenn die für die Verarbeitung der Anfrage erforderliche Zeit im Vergleich zur Dauer der Initialisierung der DTM-Instanz gering ist. Wenn die Anfrage fehlschlägt, wird die DTM-Instanz beendet.</p> <p>Muss eine Ganzzahl sein. Eine negative Ganzzahl bedeutet, dass die DTM-Keep Alive-Zeit für den Data Integration Service verwendet wird. 0 bedeutet, dass der Data Integration Service die DTM-Instanz nicht im Speicher beibehält. Standardwert ist -1.</p>

# KAPITEL 40

## infacmd xrf-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [generateReadableViewXML, 1307](#)
- [updateExportXML, 1308](#)

### generateReadableViewXML

Generiert eine lesbare XML-Datei aus einer Export-XML-Datei. Die Export-XML-Datei kann Inhalt aus exportierten Domänen oder aus dem Modellrepository enthalten.

Der Befehl „infacmd xrf generateReadableViewXML“ vereinfacht den Prozess der Bearbeitung einer Export-XML-Datei, indem die Werte, die Sie bearbeiten können, verfügbar gemacht werden. Verwenden Sie die lesbare XML-Datei, um die aus der XML-Exportdatei generierten Werte zu ändern. Wenn Sie beispielsweise eine im Modellrepository gespeicherte Zuordnung exportieren, können Sie die Namen von Spalten ändern oder die Genauigkeit und Skalierung von Datentypen bearbeiten. Wenn Sie strukturelle Änderungen an Werten in der XML-Exportdatei vornehmen möchten, verwenden Sie das Administrator Tool oder das Developer Tool, je nachdem, ob Sie den Inhalt von Domänen oder von Modellrepositorys exportiert haben.

Der Befehl infacmd xrf generateReadableViewXML verwendet die folgende Syntax:

```
generateReadableViewXML  
  
<-SourceExportFile|-sxf> source_export_file  
  
<-TargetFile|-tf> target_file_Name
```

In der folgenden Tabelle werden infacmd xrf generateReadableViewXML-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-SourceExportFile -sxf	source_export_file	Erforderlich. Pfad und Dateiname der XML-Exportdatei.
-TargetFile -tf	target_file_Name	Erforderlich. Pfad und Dateiname der lesbaren XML-Datei.

# updateExportXML

Aktualisiert eine Export-XML-Datei mit den Änderungen an der entsprechenden lesbaren XML-Datei. Sie können eine lesbare XML-Datei, die Inhalt aus dem Model Repository enthält, aktualisieren und die Export-XML-Datei mit den Änderungen erneut generieren.

Der `infacmd xrf updateExportXML`-Befehl verwendet die folgende Syntax:

```
updateExportXML  
  
<SourceExportFile|-sxf> source_file  
<generatedViewFile|-vf> view_file  
<TargetFile|-tf> target_file_Name
```

In der folgenden Tabelle werden `infacmd xrf updateExportXML`-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-SourceExportFile -sxf	source_file	Erforderlich. Pfad und Dateiname der XML-Exportdatei.
-generatedViewFile -vf	view_file	Erforderlich. Pfad und Dateiname der lesbaren XML-Datei, die die erforderlichen Änderungen enthält.
-TargetFile -tf	target_file_Name	Erforderlich. Pfad und Dateiname der aktualisierten XML-Exportdatei.



# KAPITEL 41

## infacmd-Steuerdateien

Dieses Kapitel umfasst die folgenden Themen:

- [infacmd-Steuerdateien - Übersicht, 1309](#)
- [Konfiguration von Steuerdateien, 1309](#)
- [Exportsteuerdateien, 1310](#)
- [Importsteuerdateien, 1315](#)
- [Regeln und Richtlinien für Steuerdateien, 1323](#)
- [Steuerdatei-Beispiele für Domänenobjekte, 1324](#)
- [Steuerdatei-Beispiele für Model Repository-Objekte, 1325](#)

## infacmd-Steuerdateien - Übersicht

Wenn Sie mit dem infacmd-Befehlszeilenprogramm Objekte exportieren und importieren, können Sie mit einer Kontrolldatei die Objekte filtern, die den Befehl exportieren oder importieren.

Sie können die folgenden Steuerdateien mit infacmd verwenden:

- Exportsteuerdatei. Verwenden Sie eine Exportsteuerdatei, um die Objekte anzugeben, die aus der Domäne oder aus dem Modellrepository in eine Exportdatei exportiert werden sollen.
- Importsteuerdatei. Verwenden Sie eine Importsteuerdatei, um die Objekte anzugeben, die aus der Exportdatei in die Domäne oder das Modellrepository importiert werden sollen.

Wenn Sie während des Exports keine Exportsteuerdatei verwenden, werden die aus der Domäne oder dem angegebenen Modellrepository-Projekt exportierten Objekte nicht von infacmd gefiltert. Wenn Sie während des Imports in die Domäne keine Importsteuerdatei verwenden, importiert infacmd alle in der Exportdatei enthaltenen Objekte. Wenn Sie während des Imports in das Modellrepository keine Importsteuerdatei verwenden, importiert infacmd alle im angegebenen Projekt in der Exportdatei enthaltenen Objekte.

## Konfiguration von Steuerdateien

Eine Steuerdatei ist eine XML-Datei, die auf einer Export- oder Import-Schemadatei basiert. Sie können eine Steuerdatei basierend auf den folgenden Schemadateien erstellen:

- exportControl.xsd. Legt das Layout und die Syntax der Export-Steuerdateien fest.
- importControl.xsd. Legt das Layout und die Syntax der Import-Steuerdateien fest.

Sie können in folgendem Installationsverzeichnis auf die Schemadateien als Teil der oie-util.jar zugreifen:

```
<InformaticaInstallationDir>/services/shared/jars/shapp
```

Um aus der Befehlszeile auf exportControl.xsd und importControl.xsd zuzugreifen, wechseln Sie zum Speicherort von oie-util.jar und extrahieren die JAR-Datei mit dem folgenden Befehl:

```
jar -xvf <jar_name>
```

Sie können die Datei oie-util.jar auch mit Packprogrammen wie WinRAR extrahieren oder die XSD-Dateien aus der Datei oie-util.jar mit dem Java-Decompiler anzeigen, um auf die Schemadateien zuzugreifen.

Zum Erstellen einer Export-Steuerdatei erstellen Sie eine XML-Datei basierend auf der exportControl.xsd-Schemadatei. Die Datei muss mit einer XML-Deklaration und dem Speicherort der gehosteten Schemadatei im exportParams-Root-Element beginnen. Beziehen Sie die folgenden Zeilen in der Datei ein:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
...
</exportParams>
```

Zum Erstellen einer Import-Steuerdatei erstellen Sie eine XML-Datei basierend auf der importControl.xsd-Schemadatei. Die Datei muss mit einer XML-Deklaration und dem Speicherort der gehosteten Schemadatei im importParams-Root-Element beginnen. Beziehen Sie die folgenden Zeilen in der Datei ein:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
...
</importParams>
```

Binden Sie die verbleibenden Elemente und Attribute in die XML-Datei basierend auf den Objekten ein, die Sie exportieren oder importieren möchten.

## Benennungskonventionen für Steuerdateien

Verwenden Sie einen eindeutigen Dateinamen für die Steuerdateien.

Fügen Sie jedem Dateinamen ein Präfix hinzu, um anzugeben, ob es sich um eine Export- oder Importsteuerdatei handelt. Verwenden Sie zum Beispiel die folgenden vorgeschlagenen Benennungskonventionen:

- ecf\_<file\_name>.xml für Exportsteuerdateien
- icf\_<file\_name>.xml für Importsteuerdateien

In Steuerdateien für Domänenobjekte können Sie außerdem den für den Export oder Import vorgesehenen Objekttyp im Dateinamen angeben.

## Exportsteuerdateien

Eine Exportsteuerdatei ist eine XML-Datei, die Sie mit infacmd-Befehlen verwenden. Die Steuerdatei filtert die Objekte, die infacmd aus einer Domäne oder einem Modellrepository exportiert.

Sie können eine Exportsteuerdatei mit den folgenden Befehlen verwenden:

### **infacmd isp ExportDomainObjects**

Exportiert native Benutzer, native Gruppen, Rollen, Verbindungen und Cluster-Konfigurationen aus der Domäne in eine Exportdatei im XML-Format. Wenn Sie eine Exportsteuerdatei für den Befehl angeben, filtern Sie die Objekte, die Sie exportieren möchten. Verwenden Sie zum Beispiel eine Steuerdatei zum

Exportieren aller Objekte, die nach einem bestimmten Datum erstellt wurden, oder zum Exportieren von Verbindungen (aber keine anderen Objekttypen).

#### infacmd oie ExportObjects

Exportiert alle Modellrepository-Objekttypen aus einem angegebenen Projekt in eine Exportdatei im XML-Format. Wenn Sie eine Exportsteuerdatei für den Befehl angeben, filtern Sie die Objekte, die Sie exportieren möchten. Verwenden Sie zum Beispiel eine Steuerdatei zum Exportieren aller Objekte, die von einem bestimmten Benutzer erstellt wurden, oder zum Exportieren bestimmter Objekttypen in das Projekt.

Infacmd exportiert keine leeren Ordner. Beim Exportieren von Modellrepository-Objekten exportiert infacmd ebenfalls die abhängigen Objekte. Ein abhängiges Objekt ist ein Objekt, das von einem anderen Objekt verwendet wird. Abhängige Objekte können in demselben oder in anderen Projekten vorhanden sein.

Eine Exportsteuerdatei verwendet andere Parameter basierend darauf, ob Sie die Datei zum Exportieren von Domänenobjekten oder Modellrepository-Objekten konfigurieren.

## Export-Steuerdatei-Parameter für Domänenobjekte

Verwenden Sie die Export-Steuerdatei-Parameter zum Konfigurieren der Objekte, die Sie aus der Domäne exportieren möchten.

Eine Export-Steuerdatei für Domänenobjekte kann die folgenden Elemente enthalten:

- exportParams. Kann mehrere objectList-Elemente enthalten.
- objectList. Enthält Attribute zum Filtern der Objekte nach Typ. Kann mehrere Objektelemente enthalten.
- object. Enthält ein Attribut zum Filtern von Objekten nach Namen.

In der folgenden Tabelle werden die Export-Steuerdateielemente aufgelistet, die konfigurierbare Attribute enthalten:

Element	Attributname	Attributbeschreibung
objectList	type	Erforderlich. Typ der zu exportierenden Domäne. Geben Sie einen der folgenden Werte an: <ul style="list-style-type: none"><li>- Benutzer</li><li>- Gruppe</li><li>- Role</li><li>- Cluster-Konfiguration.</li><li>- Connection</li></ul> Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
objectList	createdBefore	Optional. Datum und Uhrzeit. Exportiert Objekte des angegebenen Typs, die vor diesem Datum und dieser Uhrzeit erstellt wurden. Geben Sie das Datum und die Uhrzeit in folgendem Format ein:  yyyy-MM-dd HH:mm:ssZ
objectList	createdAfter	Optional. Datum und Uhrzeit. Exportiert Objekte des angegebenen Typs, die nach diesem Datum und dieser Uhrzeit erstellt wurden. Geben Sie das Datum und die Uhrzeit in folgendem Format ein:  yyyy-MM-dd HH:mm:ssZ

Element	Attributname	Attributbeschreibung
objectList	lastUpdatedBefore	Optional. Datum und Uhrzeit. Exportiert Objekte des angegebenen Typs, die vor diesem Datum und dieser Uhrzeit aktualisiert wurden. Geben Sie das Datum und die Uhrzeit in folgendem Format ein:  yyyy-MM-dd HH:mm:ssZ
objectList	lastUpdatedAfter	Optional. Datum und Uhrzeit. Exportiert Objekte des angegebenen Typs, die nach diesem Datum und dieser Uhrzeit aktualisiert wurden. Geben Sie das Datum und die Uhrzeit in folgendem Format ein:  yyyy-MM-dd HH:mm:ssZ
object	name	Erforderlich. Name des zu exportierenden Objekts. Wenn das enthaltene objectList-Element ein time-Attribut umfasst, exportiert infacmd Objekte, die mit dem angegebenen Objektnamen und dem Zeitfilter übereinstimmen. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.

## Export-Steuerdatei-Beispiel für Domänenobjekte

Der folgende Code zeigt ein Beispiel einer Export-Steuerdatei für Domänenobjekte:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">

  <!-- Export a specific connection. -->
  <objectList type="connection" >
    <object name="connection1" />
  </objectList>

  <!-- Export groups created before the specified date and time. -->
  <objectList type="group" createdBefore="2010-11-12 10:00:00 +0530" />

  <!-- Export role1 and role2 if created after the specified date and time. -->
  <objectList type="role" createdAfter="2010-12-25 10:00:00 +0530">
    <object name="role1" />
    <object name="role2" />
  </objectList>

  <!-- Export all users. -->
  <objectList type="user" />
</exportParams>
```

## Exportsteuerdateiparameter für Modellrepository-Objekte

Verwenden Sie die Exportsteuerdateiparameter zum Konfigurieren der Objekte, die Sie aus dem Modellrepository exportieren möchten.

Eine Exportsteuerdatei für Modellrepository-Objekte kann die folgenden Elemente enthalten:

- exportParams. Kann ein einzelnes folders-Element enthalten.
- folders. Kann mehrere folder-Elemente enthalten.
- folder. Enthält Attribute zum Filtern von Objekten in einem angegebenen Ordner. Kann mehrere objectList-Elemente enthalten.
- objectList. Enthält Attribute zum Filtern der Objekte nach Typ. Kann mehrere Objektelemente enthalten.
- object. Enthält ein Attribut zum Filtern von Objekten nach Namen.

In der folgenden Tabelle werden die konfigurierbaren Attribute für das Ordner-element in der Exportsteuerdatei beschrieben:

Attributname	Attributbeschreibung
Pfad	<p>Optional. Pfad des Ordners, der die zu exportierenden Objekte enthält. Verwenden Sie das folgende Format:</p> <pre>"/&lt;folder_name&gt;/&lt;folder_name&gt;"</pre> <p>Wenn beispielsweise ein Projekt einen Ordner mit dem Namen „F1“ enthält, ist „/F1“ der Ordnerpfad von F1. Um alle Objekte im Projekt zu exportieren, geben Sie „/“ an. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden. Standardwert ist „/“.</p>
recursive	<p>Optional. Zeigt an, ob Objekte aus Unterordnern des angegebenen Ordners exportiert werden sollen. Mit der Einstellung „true“ findet ein Export aus Unterordnern statt. Gültige Werte sind „true“ und „false“. Bei diesem Wert muss die Groß-/Kleinschreibung beachtet werden. Standardwert ist „true“.</p>
auswählen	<p>Optional. Zeigt an, ob infacmd alle übrigen Objekte im angegebenen Ordner exportiert, wenn Sie ein objectList-Element für den Ordner definieren. Bei Auswahl von „all“ werden alle übrigen Objekte exportiert. Zum Beispiel exportieren die folgenden Zeilen Zuordnungen, die von user1 erstellt wurden. Die Zeilen exportieren alle übrigen Objekte im angegebenen Ordner:</p> <pre>&lt;folder path="/Testfolder" select="all"&gt;   &lt;objectList type="Mapping" createdBy="user1" /&gt; &lt;/folder&gt;</pre> <p>Wenn Sie ein objectList-Element definieren und das select-Attribut nicht verwenden, exportiert infacmd Objekte in Übereinstimmung mit den in objectList definierten Attributen. Zum Beispiel exportieren die folgenden Zeilen Zuordnungen, die von user1 im angegebenen Ordner erstellt wurden:</p> <pre>&lt;folder path="/Testfolder"&gt;   &lt;objectList type="Mapping" createdBy="user1" /&gt; &lt;/folder&gt;</pre> <p>Wenn Sie kein objectList-Element für den Ordner definieren, ist „all“ der Standardwert des ausgewählten Attributs. Zum Beispiel exportiert die folgende Zeile alle Objekte in den angegebenen Ordner:</p> <pre>&lt;folder path="/Testfolder" /&gt;</pre> <p>Gültiger Wert ist „all“.</p>
createdBy	<p>Optional. Benutzername. Exportiert von diesem Benutzer erstellte Objekte. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.</p>
createdBefore	<p>Optional. Datum und Uhrzeit. Exportiert vor diesem Datum und dieser Uhrzeit erstellte Objekte. Geben Sie das Datum und die Uhrzeit in folgendem Format ein:</p> <pre>yyyy-MM-dd HH:mm:ssZ</pre>
createdAfter	<p>Optional. Datum und Uhrzeit. Exportiert nach diesem Datum und dieser Uhrzeit erstellte Objekte. Geben Sie das Datum und die Uhrzeit in folgendem Format ein:</p> <pre>yyyy-MM-dd HH:mm:ssZ</pre>
lastUpdatedBefore	<p>Optional. Datum und Uhrzeit. Exportiert vor diesem Datum und dieser Uhrzeit aktualisierte Objekte. Geben Sie das Datum und die Uhrzeit in folgendem Format ein:</p> <pre>yyyy-MM-dd HH:mm:ssZ</pre>

Attributname	Attributbeschreibung
lastUpdatedAfter	Optional. Datum und Uhrzeit. Exportiert nach diesem Datum und dieser Uhrzeit aktualisierte Objekte. Geben Sie das Datum und die Uhrzeit in folgendem Format ein:  yyyy-MM-dd HH:mm:ssZ
lastUpdatedBy	Optional. Benutzername. Exportiert Objekte, die von diesem Benutzer zuletzt aktualisiert wurden. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.

In der folgenden Tabelle werden die konfigurierbaren Attribute für das objectList-Element in der Exportsteuerdatei beschrieben:

Attributname	Attributbeschreibung
Typ	Erforderlich. Typ des aus dem angegebenen Ordnerpfad zu exportierenden Modellrepository-Objekts. Gültige Werte beinhalten alle Objekttypen im Modellrepository. Sie können den Objekttyp in der Ansicht „Eigenschaften“ im Developer-Tool anzeigen. Beispielsweise können Sie „Relationales Datenobjekt“ oder „Profil“ eingeben. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
createdBy	Optional. Benutzername. Exportiert Objekte des angegebenen Typs, die von diesem Benutzer erstellt wurden. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
createdBefore	Optional. Datum und Uhrzeit. Exportiert Objekte des angegebenen Typs, die vor diesem Datum und dieser Uhrzeit erstellt wurden. Geben Sie das Datum und die Uhrzeit in folgendem Format ein:  yyyy-MM-dd HH:mm:ssZ
createdAfter	Optional. Datum und Uhrzeit. Exportiert Objekte des angegebenen Typs, die nach diesem Datum und dieser Uhrzeit erstellt wurden. Geben Sie das Datum und die Uhrzeit in folgendem Format ein:  yyyy-MM-dd HH:mm:ssZ
lastUpdatedBefore	Optional. Datum und Uhrzeit. Exportiert Objekte des angegebenen Typs, die vor diesem Datum und dieser Uhrzeit aktualisiert wurden. Geben Sie das Datum und die Uhrzeit in folgendem Format ein:  yyyy-MM-dd HH:mm:ssZ
lastUpdatedAfter	Optional. Datum und Uhrzeit. Exportiert Objekte des angegebenen Typs, die nach diesem Datum und dieser Uhrzeit aktualisiert wurden. Geben Sie das Datum und die Uhrzeit in folgendem Format ein:  yyyy-MM-dd HH:mm:ssZ
lastUpdatedBy	Optional. Benutzername. Exportiert Objekte des angegebenen Typs, die von diesem Benutzer zuletzt aktualisiert wurden. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.

In der folgenden Tabelle wird das konfigurierbare Attribut für das Objektelement in der Exportsteuerdatei beschrieben:

Attributname	Attributbeschreibung
name	Erforderlich. Name des zu exportierenden Objekts. Wenn das einbezogene objectList-Element ein user- oder time-Attribut enthält, exportiert infacmd Objekte, die mit dem angegebenen Objektnamen und dem Benutzer- oder Zeitfilter übereinstimmen. Bei diesem Wert muss die Groß-/ Kleinschreibung beachtet werden.

## Exportsteuerdateibeispiel für Modellrepository-Objekte

Der folgende Code zeigt ein Beispiel einer Exportsteuerdatei für Modellrepository-Objekte:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
  <folders>

    <!-- Consider exporting all objects in the project. Do not export from subfolders. -->
    <folder recursive="false" select="all">

      <!-- Export mapping1 if created by the specified user. -->
      <objectList type="Mapping" createdBy="user1">
        <object name="mapping1"/>
      <!-- Export all other mappings. -->
      </objectList>

      <!-- Export Aggregator transformations created by the specified user. -->
      <objectList type="Aggregator" createdBy="user1" />

      <!-- Export all remaining objects. -->
    </folder>
  </folders>
</exportParams>
```

# Importsteuerdateien

Eine Importsteuerdatei ist eine XML-Datei, die Sie mit infacmd-Befehlen verwenden. Die Steuerdatei filtert die Objekte, die infacmd aus einer Exportdatei in eine Domäne oder ein Modellrepository importiert.

Sie können eine Importsteuerdatei mit den folgenden Befehlen verwenden:

### infacmd isp ImportDomainObjects

Importiert native Benutzer, native Gruppen, Rollen, Verbindungen und Cluster-Konfigurationen aus einer Exportdatei in eine Domäne. Wenn Sie eine Importsteuerdatei für den Befehl angeben, können Sie die folgenden Aufgaben abschließen:

- Filtern der Objekte, die Sie importieren möchten (Verwenden Sie zum Beispiel die Steuerdatei zum Importieren eines bestimmten Objekttyps.)
- Konfigurieren von Konfliktlösungsstrategien für bestimmte Objekttypen oder Objekte

### infacmd oie ImportObjects

Importiert Modellrepository-Objekte aus einer Exportdatei in ein Modellrepository. Wenn Sie eine Importsteuerdatei für den Befehl angeben, können Sie die folgenden Aufgaben abschließen:

- Filtern der Objekte, die Sie importieren möchten (Verwenden Sie zum Beispiel die Steuerdatei zum Importieren eines bestimmten Objekttyps.)
- Konfigurieren von Konfliktlösungsstrategien für bestimmte Objekttypen oder Objekte
- Zuordnen von Verbindungen im Quell-Repository zu Verbindungen im Target-Repository

Abhängige Modellrepository-Objekte können sich in verschiedenen Ordnern oder Projekten befinden. Sie müssen alle abhängigen Objekte mithilfe von folderMap-Elementen in die Importsteuerdatei einbeziehen. Andernfalls kann der Import mit einer Fehlermeldung fehlschlagen, da das Target-Repository kein abhängiges Objekt enthält.

Beim Importieren der Objekte können Sie eine Konfliktlösungsstrategie über die Befehlszeile oder Steuerdatei definieren. Die Steuerdatei hat Vorrang, wenn Sie eine Konfliktlösung in der Befehlszeile und der Steuerdatei definieren. Der Import schlägt fehl, wenn ein Konflikt auftritt und Sie keine Konfliktlösungsstrategie definiert haben.

Wenn Sie die Umbenennungs-Konfliktlösungsstrategie definieren, können Sie einen Namen in der Steuerdatei für ein bestimmtes Objekt angeben. Alternativ dazu kann infacmd durch Anhängen einer laufenden Nummer an das Ende des Namens einen Namen generieren.

Eine Importsteuerdatei verwendet andere Parameter basierend darauf, ob Sie die Datei zum Importieren von Domänenobjekten oder Modellrepository-Objekten konfigurieren.

## Import-Steuerdatei-Parameter für Domänenobjekte

Verwenden Sie die Import-Steuerdatei-Parameter zum Konfigurieren der Objekte, die Sie aus einer XML-Datei in die Domäne importieren möchten.

Eine Import-Steuerdatei für Domänenobjekte kann die folgenden Elemente enthalten:

- importParams. Kann mehrere objectList-Elemente enthalten.
- objectList. Enthält Attribute zum Filtern der Objekte nach Typ. Kann mehrere Objektelemente enthalten.
- object. Enthält Attribute zum Filtern der Objekte nach Namen.



In der folgenden Tabelle werden die Import-Steuerdateielemente aufgelistet, die konfigurierbare Attribute enthalten:

Element	Attributname	Attributbeschreibung
objectList	type	<p>Erforderlich. Typ des Domänenobjekts, das Sie importieren möchten. Geben Sie einen der folgenden Werte an:</p> <ul style="list-style-type: none"> <li>- Benutzer</li> <li>- Gruppe</li> <li>- Role</li> <li>- Cluster-Konfiguration</li> <li>- Connection</li> </ul> <p>Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.</p>
objectList	select	<p>Optional. Zeigt an, ob infacmd alle übrigen Objekte des angegebenen Typs importiert, wenn Sie ein object-Element für objectList definieren. Bei Auswahl von „all“ werden alle übrigen Objekte importiert. Zum Beispiel importieren die folgenden Zeilen Group1 mit einer Reuse-Lösungsstrategie. Die Zeilen importieren alle übrigen Gruppen mit einer Merge-Lösungsstrategie:</p> <pre>&lt;objectList type="group" select="all" resolution="merge"&gt;   &lt;object name="Group1" resolution="reuse" /&gt; &lt;/objectList&gt;</pre> <p>Wenn Sie ein Objektelement definieren und das select-Attribut nicht verwenden, importiert infacmd Objekte in Übereinstimmung mit den im object-Element definierten Attributen. Zum Beispiel importieren die folgenden Zeilen Group1 mit einer Merge-Lösungsstrategie.</p> <pre>&lt;objectList type="group" resolution="merge"&gt;   &lt;object name="Group1" /&gt; &lt;/objectList&gt;</pre> <p>Wenn Sie kein object-Element für objectList definieren, ist „all“ der Standardwert des ausgewählten Attributs. Zum Beispiel importieren die folgenden Zeilen alle Gruppen mit einer Merge-Lösungsstrategie.</p> <pre>&lt;objectList type="group" resolution="merge" /&gt;</pre> <p>Gültiger Wert ist „all“.</p>
objectList	resolution	<p>Optional. Lösungsstrategie bei Auftreten eines Namenskonflikts. Gilt für alle Objekte des angegebenen Typs. Geben Sie einen der folgenden Werte an:</p> <ul style="list-style-type: none"> <li>- Replace. Ersetzen Sie das Target-Objekt mit dem Quellobjekt.</li> <li>- Rename. Benennen Sie das Quellobjekt mit einem generierten Namen um und importieren Sie es anschließend.</li> </ul> <p>Sie können die Option Rename nicht mit dem Cluster-Konfigurationstyp verwenden.</p> <ul style="list-style-type: none"> <li>- Reuse. Verwenden Sie das Objekt in der Target-Domäne wieder.</li> <li>- Merge. Führen Sie die Objekte in einem Objekt zusammen. Diese Option kann für Gruppen verwendet werden.</li> </ul> <p>Bei diesen Werten muss die Groß-/Kleinschreibung nicht beachtet werden.</p>
object	name	<p>Erforderlich. Name eines bestimmten zu importierenden Objekts des angegebenen Objekttyps. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.</p>

Element	Attributname	Attributbeschreibung
object	resolution	Optional. Lösungsstrategie bei Auftreten eines Namenskonflikts für dieses Objekt. Geben Sie einen der folgenden Werte an: <ul style="list-style-type: none"> <li>- Replace. Ersetzen Sie das Target-Objekt mit dem Quellobjekt.</li> <li>- Rename. Benennen Sie das Quellobjekt um und importieren Sie es anschließend.</li> </ul> <p>Sie können die Option Rename nicht mit dem Cluster-Konfigurationstyp verwenden.</p> <ul style="list-style-type: none"> <li>- Reuse. Verwenden Sie das Objekt in der Target-Domäne wieder.</li> <li>- Merge. Führen Sie die Objekte in einem Objekt zusammen. Diese Option kann für Gruppen verwendet werden.</li> </ul> <p>Bei diesen Werten muss die Groß-/Kleinschreibung nicht beachtet werden.</p>
object	renameTo	Optional. Zu verwendender Name, wenn Rename als Konfliktlösungsstrategie dient. Wenn Sie keinen Namen festlegen, generiert infacmd einen Namen durch Anhängen einer Nummer an das Ende des Namens. Infacmd ignoriert den Wert, wenn keine Konflikte auftreten oder wenn es sich bei der Konfliktlösungsstrategie nicht um Rename handelt.
object	renamedTo	Optional. Zu verwendende ID-Zeichenfolge, wenn Sie ein Verbindungsobjekt importieren und Rename als Konfliktlösungsstrategie dient. Wenn Sie keine Verbindungs-ID angeben, generiert infacmd eine ID durch Anhängen einer Nummer an das Ende der Verbindungs-ID. Infacmd ignoriert den Wert, wenn keine Konflikte auftreten oder wenn es sich bei der Konfliktlösungsstrategie nicht um Rename handelt.

## Import-Steuerdatei-Beispiel für Domänenobjekte

Der folgende Code zeigt ein Beispiel einer Import-Steuerdatei für Domänenobjekte:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">

  <!-- Import all connections, roles, and users. -->
  <objectList type="connection" resolution="replace" />
  <objectList type="role" resolution="reuse" />
  <objectList type="user" resolution="rename" />

  <!-- Import specific groups. -->
  <objectList type="group">
    <object name="g1" resolution="replace" />
    <object name="g2" resolution="merge" />
  </objectList>
</importParams>
```

## Importsteuerdateiparameter für Modellrepository-Objekte

Verwenden Sie die Importsteuerdateiparameter zum Konfigurieren der Objekte, die Sie aus einer XML-Datei in das Modellrepository importieren möchten.

Eine Importsteuerdatei für Modellrepository-Objekte können die folgenden Elemente enthalten:

- importParams. Können ein einzelnes folderMaps-Element in einem einzelnen connectionInfo-Element enthalten.
- folderMaps. Kann Elemente aus mehreren folderMap-Elementen enthalten.
- folderMap. Enthält Attribute zum Filtern von Objekten in einem angegebenen Ordner. Kann mehrere objectList-Elemente enthalten.

- **objectList.** Enthält Attribute zum Filtern der Objekte nach Typ. Kann mehrere Objektelemente enthalten.
- **object.** Enthält Attribute zum Filtern der Objekte nach Namen.
- **connectionInfo.** Kann ein einzelnes rebindMap-Element enthalten.
- **rebindMap.** Kann mehrere rebind-Elemente enthalten.
- **rebind.** Enthält Attribute zum Zuordnen von Verbindungen im Quell-Repository zu Verbindungen im Target-Repository.

In der folgenden Tabelle werden die konfigurierbaren Attribute für das folderMap-Element in der Importsteuerdatei beschrieben:

Attributname	Attributbeschreibung
sourceProject	Erforderlich. Name des Quellprojekts in der Exportdatei, das die zu importierenden Objekte enthält. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
sourceFolderPath	Optional. Pfad des Quellordners in der Exportdatei, der die zu importierenden Objekte enthält. Verwenden Sie das folgende Format: "/<folder_name>/<folder_name>" Wenn beispielsweise ein Projekt einen Ordner mit dem Namen „F1“ enthält, ist „/F1“ der Ordnerpfad von F1. Um alle Objekte im Projekt zu importieren, geben Sie „/“ an. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden. Standardwert ist „/“.
targetProject	Erforderlich. Name des Projekts im Target-Repository, in das Objekte importiert werden sollen. Das Projekt muss im Repository vorhanden sein, bevor Sie diese Objekte importieren. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
targetFolderPath	Optional. Pfad des Ordners im Target-Repository, in das Sie Objekte importieren möchten. Verwenden Sie das folgende Format: "/<folder_name>/<folder_name>" Wenn beispielsweise ein Projekt einen Ordner mit dem Namen „F1“ enthält, ist „/F1“ der Ordnerpfad von F1. Um alle Objekte in das Target-Projekt zu importieren, geben Sie „/“ an. Der Ordner muss im Repository vorhanden sein, bevor Sie diese Objekte importieren. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden. Standardwert ist „/“.
recursive	Optional. Zeigt an, ob Objekte aus Unterordnern des angegebenen Ordners importiert werden sollen. Mit der Einstellung „true“ findet ein Import aus Unterordnern statt. Gültige Werte sind „true“ und „false“. Bei diesem Wert muss die Groß-/Kleinschreibung beachtet werden. Standardwert ist „true“.

Attributname	Attributbeschreibung
auswählen	<p>Optional. Zeigt an, ob infacmd alle übrigen Objekte im angegebenen Projekt importiert, wenn Sie ein objectList-Element für folderMap definieren. Bei Auswahl von „all“ werden alle übrigen Objekte importiert. Zum Beispiel importieren die folgenden Zeilen Zuordnungen mit einer Reuse-Lösungsstrategie. Die Zeilen importieren alle übrigen Objekte mit einer Replace-Lösungsstrategie:</p> <pre>&lt;folderMap sourceProject="p1" targetProject="p2" select="all" resolution="replace"&gt;   &lt;objectList type="Mapping" resolution="reuse" /&gt; &lt;/folderMap&gt;</pre> <p>Wenn Sie ein objectList-Element definieren und das select-Attribut nicht verwenden, importiert infacmd Objekte in Übereinstimmung mit den in objectList definierten Attributen. Zum Beispiel importieren die folgenden Zeilen Zuordnungen mit einer Replace-Lösungsstrategie:</p> <pre>&lt;folderMap sourceProject="p1" targetProject="p2" resolution="replace"&gt;   &lt;objectList type="Mapping" /&gt; &lt;/folderMap&gt;</pre> <p>Wenn Sie kein objectList-Element für folderMap definieren, wird der Standardwert „all“ verwendet. Zum Beispiel importiert die folgende Zeile alle Objekte mit einer Replace-Lösungsstrategie:</p> <pre>&lt;folderMap sourceProject="p1" targetProject="p2" resolution="replace" /&gt;</pre> <p>Gültiger Wert ist „all“.</p>
resolution	<p>Optional. Lösungsstrategie bei Auftreten eines Namenskonflikts. Gilt für alle Objekte in diesem Ordner. Geben Sie einen der folgenden Werte an:</p> <ul style="list-style-type: none"> <li>- Rename. Benennen Sie das Quellobjekt mit einem generierten Namen um und importieren Sie es anschließend.</li> <li>- Replace. Ersetzen Sie das Target-Objekt mit dem Quellobjekt.</li> <li>- Reuse. Verwenden Sie das Objekt im Modellrepository wieder.</li> <li>- Keine.</li> </ul> <p>Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden. Der Standardwert ist „Keine“.</p>

In der folgenden Tabelle werden die konfigurierbaren Attribute für das objectList-Element in der Importsteuerdatei beschrieben:

Attributname	Attributbeschreibung
Typ	Erforderlich. Typ des Modellrepository-Objekts, das in den angegebenen Ordnerpfad importiert werden soll. Gültige Werte beinhalten alle Objekttypen im Modellrepository. Sie können den Objekttyp in der Ansicht „Eigenschaften“ im Developer-Tool anzeigen. Beispielsweise können Sie „Relationales Datenobjekt“ oder „Profil“ eingeben. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
auswählen	<p>Optional. Zeigt an, ob infacmd alle übrigen Objekte des angegebenen Typs importiert, wenn Sie ein object-Element für objectList definieren. Bei Auswahl von „all“ werden alle übrigen Objekte importiert. Zum Beispiel importieren die folgenden Zeilen MyMapping mit einer Reuse-Lösungsstrategie. Die Zeilen importieren alle übrigen Zuordnungen mit einer Replace-Lösungsstrategie:</p> <pre>&lt;folderMap sourceProject="p1" targetProject="p2"&gt;   &lt;objectList type="Mapping" select="all" resolution="replace"&gt;     &lt;object name="MyMapping" resolution="reuse" /&gt;   &lt;/objectList&gt; &lt;/folderMap&gt;</pre> <p>Wenn Sie ein Objektelelement definieren und das select-Attribut nicht verwenden, importiert infacmd Objekte in Übereinstimmung mit den im Objektelelement definierten Attributen. Zum Beispiel importieren die folgenden Zeilen die Zuordnung namens MyMapping mit einer Replace-Lösungsstrategie:</p> <pre>&lt;folderMap sourceProject="p1" targetProject="p2"&gt;   &lt;objectList type="Mapping" resolution="replace"&gt;     &lt;object name="MyMapping" /&gt;   &lt;/objectList&gt; &lt;/folderMap&gt;</pre> <p>Wenn Sie kein object-Element für objectList definieren, wird der Standardwert „all“ verwendet. Zum Beispiel importieren die folgenden Zeilen alle Zuordnungen mit einer Replace-Lösungsstrategie:</p> <pre>&lt;folderMap sourceProject="p1" targetProject="p2"&gt;   &lt;objectList type="Mapping" resolution="replace" /&gt; &lt;/folderMap&gt;</pre> <p>Gültiger Wert ist „all“.</p>
resolution	<p>Optional. Lösungsstrategie bei Auftreten eines Namenskonflikts. Gilt für alle Objekte des angegebenen Typs. Geben Sie einen der folgenden Werte an:</p> <ul style="list-style-type: none"> <li>- Rename. Benennen Sie das Quellobjekt mit einem generierten Namen um und importieren Sie es anschließend.</li> <li>- Replace. Ersetzen Sie das Target-Objekt mit dem Quellobjekt.</li> <li>- Reuse. Verwenden Sie das Objekt im Modellrepository wieder.</li> <li>- Keine.</li> </ul> <p>Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden. Der Standardwert ist „Keine“.</p>

In der folgenden Tabelle werden die konfigurierbaren Attribute für das Objektelement in der Importsteuerdatei beschrieben:

Attributname	Attributbeschreibung
name	Erforderlich. Name eines bestimmten zu importierenden Objekts des angegebenen Objekttyps. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
resolution	Optional. Lösungsstrategie bei Auftreten eines Namenskonflikts für dieses Objekt. Geben Sie einen der folgenden Werte an: <ul style="list-style-type: none"> <li>- Rename. Benennen Sie das Quellobjekt um und importieren Sie es anschließend.</li> <li>- Replace. Ersetzen Sie das Target-Objekt mit dem Quellobjekt.</li> <li>- Reuse. Verwenden Sie das Objekt im Modellrepository wieder.</li> <li>- Keine.</li> </ul> Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden. Der Standardwert ist „Keine“.
renameTo	Optional. Zu verwendender Name, wenn Rename als Konfliktlösungsstrategie dient. Wenn Sie keinen Namen festlegen, generiert infacmd einen Namen durch Anhängen einer Zahl an das Ende des Namens. Infacmd ignoriert den Wert, wenn keine Konflikte auftreten oder wenn es sich bei der Konfliktlösungsstrategie nicht um Rename handelt.
renamedTo	Optional. Zu verwendender ID-String beim Importieren eines Verbindungsobjekts und wenn die Konfliktlösungsstrategie „Umbenennen“ lautet. Wenn Sie keine Verbindungs-ID angeben, generiert infacmd eine ID, indem eine Nummer an das Ende der Verbindungs-ID angehängt wird. Infacmd ignoriert den Wert, wenn keine Konflikte auftreten oder wenn es sich bei der Konfliktlösungsstrategie nicht um Rename handelt.

In der folgenden Tabelle werden die konfigurierbaren Attribute für das rebind-Element in der Importsteuerdatei beschrieben:

Attributname	Attributbeschreibung
source	Erforderlich. Name einer Quellverbindung in der Datei, die Sie importieren. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
target	Erforderlich. Name einer Verbindung im Target-Modellrepository, die der Quellverbindung zugeordnet werden soll. Standardmäßig muss die Verbindung im Zielrepository vorhanden sein, bevor Sie diese Objekte importieren. Wenn die Verbindung nicht vorhanden ist, schlägt der Import fehl. Wenn Sie infacmd ausführen, können Sie die Validierung der Zielverbindung während des Imports überspringen. Wenn Sie die Validierung der Zielverbindung überspringen, wird der Import auch dann erfolgreich ausgeführt, wenn keine Verbindung im Zielrepository vorhanden ist. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.

## Importsteuerdateibeispiel für Modellrepository-Objekte

Der folgende Code zeigt ein Beispiel einer Importsteuerdatei für Modellrepository-Objekte:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
  <folderMaps>
    <folderMap sourceProject="project1" sourceFolderPath="/f1" targetProject="project2"
      targetFolderPath="/f1" recursive="true">

      <!-- Import mapping1 with the Rename resolution strategy. -->
      <objectList type="Mapping" select="all" resolution="replace">
        <object name="mapping1" resolution="rename" renameTo="mapping1_new"/>

      <!-- Import all remaining mappings with the Replace resolution strategy. -->
    </objectList>
  </folderMap>
</folderMaps>
</importParams>
```

```

<!-- Import all Aggregator transformations with the Replace resolution strategy. -->
<objectList type="Aggregator" resolution="replace"/>

<!-- Import all Filter transformations with no resolution strategy. -->
<objectList type="Filter" resolution="none"/>
</folderMap>
</folderMaps>

<!-- Map connections in the source repository to connections in the target repository.
-->
<connectionInfo>
  <rebindMap>
    <rebind source="src_Conn1" target="tgt_Conn1"/>
    <rebind source="src_Conn2" target="tgt_Conn2"/>
  </rebindMap>
</connectionInfo>
</importParams>

```

## Regeln und Richtlinien für Steuerdateien

Überprüfen Sie die folgenden Regeln und Richtlinien, bevor Sie Steuerdateien erstellen:

- Bei Element- und Attributnamen muss die Groß-/Kleinschreibung nicht beachtet werden.
- Steuerdateien enthalten eine Hierarchie von XML-Elementen. Elemente auf verschiedenen Ebenen können dasselbe Attribut enthalten. Ein untergeordnetes Element erbt einen für das übergeordnete Element definierten Wert, wenn dasselbe Attribut nicht für das untergeordnete Element definiert ist. Die für das untergeordnete Element definierten Attributwerte überschreiben den Wert desselben Attributs, das für das übergeordnete Element definiert ist.
- Wenn ein Element mehrere Attribute definiert, exportiert oder importiert infacmd alle Objekte, die mit allen Attributfiltern übereinstimmen. Sie definieren zum Beispiel die Attribute `createdBefore` und `lastUpdatedAfter` für ein `objectList`-Element in einer Export-Steuerdatei. Infacmd exportiert Objekte des angegebenen Typs, die vor dem angegebenen Datum erstellt und nach dem angegebenen Datum zuletzt aktualisiert wurden.
- Die Werte der time-Attribute werden dabei nicht berücksichtigt. Sie legen zum Beispiel für `createdAfter` den Eintrag "2011-02-01 16:00:00-0800" in einer Export-Steuerdatei fest. Infacmd exportiert alle Objekte, die nach dem 1. Februar 2011 um 16 Uhr erstellt wurden. Infacmd exportiert alle keine Objekte, die am 1. Februar 2011 um 16 Uhr erstellt wurden.
- Sie können ein `objectList`-Element eines bestimmten Typs einmal in einer Steuerdatei für Domänenobjekte angeben. Sie geben zum Beispiel ein `objectList`-Element vom Typ "connection" an. Sie können kein anderes `objectList`-Element vom Typ "connection" in derselben Datei angeben.
- Sie können ein `objectList`-Element eines bestimmten Typs einmal in einem Ordner oder `folderMap`-Element für Model Repository-Objekte angeben. Sie geben zum Beispiel ein `objectList`-Element vom Typ "Flat File Data Object" an. Sie können kein anderes `objectList`-Element vom Typ "Flat File Data Object" in demselben Ordner oder `folderMap`-Element angeben.

# Steuerdatei-Beispiele für Domänenobjekte

Sie können Domänenobjekte filtern, um diese nach Datum/Uhrzeit zu exportieren. Sie können Domänenobjekte filtern, um diese nach Objekttyp und Objektname zu exportieren und zu importieren.

## Exportieren von Domänenobjekten nach Zeit

Um nach dem 25.12.2010 um 15:30 Uhr erstellte Benutzer zu exportieren, können Sie die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
  <objectList type="user" createdAfter="2010-12-25 10:00:00 +0530" />
</exportParams>
```

## Exportieren und Importieren von Domänenobjekten nach Typ

Um alle Benutzer, Gruppen und Rollen (aber keine Verbindungen) aus einer Domäne zu exportieren, können Sie die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
  <objectList type="group"/>
  <objectList type="role" />
  <objectList type="user" />
</exportParams>
```

Um die Benutzer und Gruppen (aber keine Rollen) in die Target-Domäne zu importieren, können Sie die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
  <objectList type="group" resolution="merge"/>
  <objectList type="user" resolution="replace" />
</importParams>
```

## Exportieren und Importieren von Domänenobjekten nach Namen

Sie möchten alle Benutzer und Benutzergruppen und die Developer- und Analyst-Rollen aus der Quelldomäne exportieren. Sie möchten bestimmte Verbindungen exportieren, wenn diese nach dem 02.01.2011 um 08:00 Uhr erstellt wurden. Sie können die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
  <objectList type="group"/>
  <objectList type="user" />
  <objectList type="role">
    <object name="Developer" />
    <object name="Analyst" />
  </objectList>
  <objectList type="connection" createdAfter="2011-02-01 16:00:00-0800">
    <object name="Connection1" />
    <object name="Connection2" />
    <object name="Connection3" />
  </objectList>
</exportParams>
```

Um alle Benutzer und Gruppen (und bestimmte Rollen und Verbindungen) in die Target-Domäne zu importieren, können Sie die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
  <objectList type="group" resolution="reuse" />
  <objectList type="user" resolution="reuse" />
  <objectList type="role">
    <object name="Developer" resolution="replace" />
    <object name="Analyst" resolution="replace" />
  </objectList>
```



```

<objectList type="connection">
  <object name="Connection1" resolution="rename" renameTo="ProdConnection1" />
  <object name="Connection2" resolution="rename" renameTo="ProdConnection2" />
  <object name="Connection3" resolution="rename" renameTo="ProdConnection3" />
</objectList>
</importParams>

```

## Steuerdatei-Beispiele für Model Repository-Objekte

Sie können den Export der Model Repository-Objekte nach Zeit oder Benutzer filtern. Sie können den Export oder Import der Model Repository-Objekte nach Objekttyp oder Objektnamen filtern.

### Exportieren von Model Repository-Objekten nach Zeit

Um alle Objekte in einem Ordner namens Folder1 zu exportieren, die vor dem 02.01.2011 um 8:00 Uhr erstellt wurden, können Sie die folgende Steuerdatei erstellen:

```

<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
  <folders>
    <folder path="/Folder1" createdBefore="2011-02-01 16:00:00-0800" />
  </folders>
</exportParams>

```

### Exportieren von Model Repository-Objekten nach Benutzer

Um alle Objekte in dem vom Administrator zuletzt aktualisierten Projekt zu exportieren, können Sie die folgende Steuerdatei erstellen:

```

<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
  <folders>
    <folder lastUpdatedBy="Administrator" />
  </folders>
</exportParams>

```

### Exportieren und Importieren von Model Repository-Objekten nach Typ

Um alle Zuordnungen aus einem Ordner namens Folder1 zu exportieren, können Sie die folgende Steuerdatei erstellen:

```

<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
  <folders>
    <folder path="/Folder1" />
      <objectList type="Mapping" />
    </folder>
  </folders>
</exportParams>

```

Sie möchten zum Beispiel alle von user2 erstellten Mappings und alle übrigen von user1 erstellen. Objekte exportieren. Das für das untergeordnete objectList-Element erstellte createdBy-Attribut überschreibt dasselbe für das übergeordnete Ordner-element definierte Attribut. Sie können die folgende Steuerdatei erstellen:

```

<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
  <folders>
    <folder path="/Folder1" select="all" createdBy="user1" />
      <objectList type="Mapping" createdBy="user2" />
    </folder>
  </folders>
</exportParams>

```

Sie möchten alle Mappings aus der Exportdatei importieren. Einige der aus Folder1 exportierten Mappings enthalten abhängige Objekte, die in Folder2 des Quell-Repositorys enthalten waren. Um abhängige Objekte zu importieren, müssen Sie alle abhängigen Objekte mithilfe von folderMap-Elementen in die Import-Steuerdatei einbeziehen. Sie möchten ebenfalls die Verbindungen im Quell-Repository zu den Verbindungen im Target-Repository zuordnen. Sie können die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
<folderMaps>
  <folderMap sourceProject="DevProject" sourceFolderPath="/Folder1"
targetProject="TestProject" targetFolderPath="/TestFolder1" resolution="reuse">
    <objectList type="Mapping" />
  </folderMap>
  <folderMap sourceProject="DevProject" sourceFolderPath="/Folder2"
targetProject="TestProject" targetFolderPath="/TestFolder2" resolution="reuse" />
</folderMaps>
<connectionInfo>
  <rebindMap>
    <rebind source="src_connection1" target="tgt_connection1" />
    <rebind source="src_connection2" target="tgt_connection2" />
  </rebindMap>
</connectionInfo>
</importParams>
```

#### Exportieren und Importieren von Model Repository-Objekten nach Name

Sie möchten eine Zuordnung namens TestMapping exportieren, die nach dem 11.11.2010 um 15:59:59 Uhr erstellt wurde. Sie möchten alle übrigen Objekte in denselben Ordner exportieren. Sie können die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
<folders>
  <folder path="/Folder1" select="all" />
    <objectList type="Mapping" createdAfter="2010-11-11 23:59:59-0800" >
      <object name="TestMapping" />
    </objectList>
  </folder>
</folders>
</exportParams>
```

Eine Exportdatei enthält Einfachdatei-Datenobjekte und relationale Datenobjekte. Sie möchten das Einfachdatei-Datenobjekt namens NewFlatFileDataObject und alle relationalen Datenobjekte aus der Exportdatei importieren. Sie können die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
<folderMaps>
  <folderMap sourceProject="SampleProject" targetProject="SampleProject"
targetFolderPath="/TestFolder">
    <objectList type="Flat File Data Object" resolution="replace" >
      <object name="NewFlatFileDataObject" />
    </objectList>
    <objectList type="Relational Data Object" resolution="replace" />
  </folderMap>
</folderMaps>
</importParams>
```

# KAPITEL 42

## infasetup-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [Verwenden von infasetup, 1328](#)
- [BackupDomain, 1329](#)
- [DefineDomain, 1332](#)
- [DefineGatewayNode, 1342](#)
- [DefineWorkerNode, 1348](#)
- [DeleteDomain, 1353](#)
- [GenerateEncryptionKey, 1356](#)
- [Hilfe, 1356](#)
- [ListDomainCiphers, 1357](#)
- [MigrateEncryptionKey, 1358](#)
- [RestoreDomain, 1359](#)
- [restoreMitKerberosLinkage, 1362](#)
- [SwitchToKerberosMode, 1363](#)
- [UpdateDomainCiphers, 1364](#)
- [updateDomainName, 1367](#)
- [UpdateGatewayNode, 1367](#)
- [UpdateKerberosAdminUser, 1373](#)
- [UpdateKerberosConfig, 1373](#)
- [updateMitKerberosLinkage, 1374](#)
- [UpdatePasswordComplexityConfig, 1376](#)
- [updateDomainSamlConfig, 1376](#)
- [UpdateWorkerNode, 1379](#)
- [upgradeDomainMetadata, 1384](#)
- [UpgradeGatewayNodeMetadata, 1386](#)
- [UnlockUser, 1388](#)
- [ValidateandRegisterFeature, 1389](#)

# Verwenden von infasetup

*infasetup* ist ein Befehlszeilenprogramm zum Verwalten von Informatica-Domänen und -Knoten.

Verwenden Sie *infasetup* zum Ändern der Domänen- und Knoteneigenschaften nach der Installation der Informatica-Dienste mit dem Informatica-Installationsprogramm. Sie können *infasetup* beispielsweise verwenden, um die Portnummer für einen Knoten zu ändern, nachdem Sie Informatica-Dienste auf dem Knoten installiert haben.

Sie können mit *infasetup* Domänen sichern, wiederherstellen, definieren und löschen sowie Knoten definieren und aktualisieren.

## Ausführen von Befehlen

*infasetup* wird über die Befehlszeile aufgerufen. Sie können Befehle direkt oder aus einem Skript, einer Batchdatei oder einem anderen Programm ausführen. Unter Windows handelt es sich bei *infasetup* um eine Batchdatei mit der Erweiterung *.bat*. Unter UNIX handelt es sich bei *infasetup* um eine Skriptdatei mit der Erweiterung *.sh*.

So führen Sie *infasetup*-Befehle aus:

1. Öffnen Sie die Eingabeaufforderung.  
Öffnen Sie unter Windows die Eingabeaufforderung als Administrator. Wenn Sie die Eingabeaufforderung nicht als Administrator öffnen, hat der Windows-Systemadministrator beim Zugriff auf Dateien im Informatica-Installationsverzeichnis möglicherweise Probleme.
2. Wechseln Sie an der Eingabeaufforderung zu dem Verzeichnis, in dem sich die ausführbare *infasetup*-Datei befindet.  
Standardmäßig wird *infasetup* im Verzeichnis `<InformaticaInstallationDir>/isp/bin` installiert.
3. Geben Sie *infasetup* unter Windows oder *infasetup.sh* unter UNIX gefolgt vom Befehlsnamen und den erforderlichen Optionen und Argumenten ein. Bei Befehlsnamen spielt die Groß- und Kleinschreibung keine Rolle.

Beispiel:

```
infasetup(.sh) command_name [-option1] argument_1 [-option2] argument_2...
```

## Befehlsoptionen

Beim Ausführen von *infasetup* geben Sie Optionen für jeden Befehl gefolgt von den erforderlichen Argumenten ein. Befehlsoptionen wird unter Missachtung der Groß-/Kleinschreibung ein Bindestrich vorangestellt. Argumente folgen der Option.

Folgender Befehl beispielsweise aktualisiert einen Arbeitsknoten mit dem Namen "Node1" und der Adresse "Host1:9090":

```
infasetup UpdateWorkerNode -nn Node1 -na Host1:9090
```

Wenn Sie eine der erforderlichen Optionen weglassen oder falsch eingeben, schlägt der Befehl fehl und von *infasetup* wird eine Fehlermeldung zurückgegeben.

## infasetup Befehlsreferenz

*infasetup* gibt die erfolgreiche oder fehlgeschlagene Ausführung eines Befehls mit einem Rückgabewert an. Rückgabewert (0) gibt an, dass der Befehl erfolgreich ausgeführt wurde. Rückgabewert (-1) gibt an, dass der Befehl fehlgeschlagen ist.

Verwenden Sie den DOS- oder UNIX-echo-Befehl unmittelbar nach Ausführung eines *infasetup*-Befehls, um den Rückgabewert für den Befehl anzuzeigen:

- An einer DOS-Shell: `echo %ERRORLEVEL%`
- An einer UNIX Bourne- oder Korn-Shell: `echo $?`
- An einer UNIX C-Shell: `echo $status`

## Verwenden von Datenbankverbindungsstrings

Einige *infasetup*-Befehle verwenden Verbindungsstrings, um eine Verbindung zur Domänen-Konfigurationsdatenbank herzustellen. Geben Sie den Host, Port und Dienstnamen der Datenbank als Teil des Verbindungsstrings an.

Sie können Verbindungsstrings mit den folgenden *infasetup*-Befehlen verwenden:

- BackupDomain
- DefineDomain
- DefineGatewayNode
- DeleteDomain
- RestoreDomain
- UpdateGatewayNode

In der folgenden Tabelle finden Sie eine Auflistung der Verbindungsstringsyntax für die einzelnen unterstützten Datenbanken:

Datenbankname	Verbindungsstring
Oracle	<b>Oracle:</b>  <code>jdbc:informatica:oracle://host_name:port;SID=sid</code>  <b>Oracle RAC:</b>  <code>jdbc:informatica:oracle://host_name:port; ServiceName=[Service Name];AlternateServers=(server2:port);LoadBalancing=true</code>
Microsoft SQL Server	<code>jdbc:informatica:sqlserver://host_name:port; SelectMethod=cursor;DatabaseName=database_name</code>
IBM DB2	<code>jdbc:informatica:db2://host_name:port; DatabaseName=database_name</code>

## BackupDomain

Sichert die Konfigurationsmetadaten für die Domäne. *infasetup* speichert die Metadaten der Backup-Domäne in einer Sicherungsdatei mit der Endung „mrep“.

Sie müssen die Domäne vor dem Ausführen dieses Befehls herunterfahren.

Wenn Sie diesen Befehl ausführen, sichert *infasetup* die Tabellen der Domänenkonfigurationsdatenbank, um die Domäne in einer anderen Datenbank wiederherzustellen. Sie müssen den Inhalt der ISP\_RUN\_LOG-Tabelle manuell sichern, um die vorherigen Arbeitsablauf- und Sitzungsprotokolle abzurufen.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, stellen Sie für „infasetup“ mehr Systemspeicher zur Verfügung. Um mehr Systemspeicher zur Verfügung zu stellen, geben Sie den -Xmx-Wert in der Umgebungsvariable INFA\_JAVA\_CMD\_OPTS an.

Der Befehl „BackupDomain“ verwendet die folgende Syntax:

```
BackupDomain

<<-DatabaseAddress|-da> database_hostname:database_port|

<-DatabaseConnectionString|-cs> database_connection_string>

[<-DatabaseUserName|-du> database_user_name]

[<-DatabasePassword|-dp> database_password]

<-DatabaseType|-dt> database_type

[<-DatabaseServiceName|-ds> database_service_name]

<-BackupFile|-bf> backup_file_name

[<-Force|-f> overwrite_file]

[<-Tablespace|-ts> tablespace_name]

[<-SchemaName|-sc> schema_name (used for Microsoft SQL Server only)]

<-DomainName|-dn> domain_name

[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]

[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]

[<-TrustedConnection|-tc> trusted_connection (used for Microsoft SQL Server only)]

[<-EncryptionKeyLocation|-kl> encryption_key_location]

[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
```

In der folgenden Tabelle werden Optionen und Argumente für „infasetup BackupDomain“ beschrieben:

Option	Argument	Beschreibung
-DatabaseAddress -da	database_hostname:database_port	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Name und Portnummer des Computers, auf dem die Konfigurationsdatenbank der Domäne gehostet wird.
-DatabaseConnectionString -cs	database_connection_string	Erforderlich, wenn Sie die Optionen -DatabaseAddress (-da) und -DatabaseServiceName (-ds) nicht verwenden. Verbindungszeichenfolge, die zum Herstellen einer Verbindung zur Konfigurationsdatenbank der Domäne verwendet wird. Geben Sie den Namen des Datenbankhosts, -ports und -diensts als Teil der Verbindungszeichenfolge ein. Setzen Sie die Verbindungszeichenfolge in Anführungszeichen.
-DatabaseUserName -du	database_user_name	Erforderlich, wenn Sie die Option -TrustedConnection (-tc) nicht verwenden. Konto für die Datenbank, die die Domänenkonfigurationsinformationen enthält.

Option	Argument	Beschreibung
-DatabasePassword -dp	database_password	Passwort aus der Datenbank für die Domänenkonfiguration des Datenbankbenutzers. Wenn Sie diese Option weglassen, verwendet <i>infasetup</i> das in der Umgebungsvariable <code>INFA_DEFAULT_DATABASE_PASSWORD</code> angegebene Passwort. Wird in der Umgebungsvariable kein Wert angegeben, müssen Sie ein Passwort unter Verwendung dieser Option eingeben.
-DatabaseType -dt	database_type	Erforderlich. Typ der Datenbank, in der die Domänenkonfigurationsmetadaten gespeichert werden. Zu den Datenbanktypen gehören: <ul style="list-style-type: none"> <li>- db2</li> <li>- oracle</li> <li>- mssqlserver</li> <li>- sybase</li> </ul>
-DatabaseServiceName -ds	database_service_name	Erforderlich, wenn Sie die Option - DatabaseConnectionString (-cs) nicht verwenden. Der Name des Datenbankdiensts. Erforderlich für Oracle-, IBM DB2- und Microsoft SQL Server-Datenbanken. Geben Sie die SID für Oracle, den Dienstnamen für IBM DB2 oder den Datenbanknamen für Microsoft SQL Server ein.
-BackupFile -bf	backup_file_name	Erforderlich. Name und Pfad der Backup-Datei. Wenn Sie keinen Dateipfad angeben, erstellt <i>infasetup</i> die Backup-Datei im aktuellen Verzeichnis.
-Force -f	-	Optional. Überschreibt die Backup-Datei, wenn eine Datei mit demselben Namen bereits vorhanden ist.
-DomainName -dn	domain_name	Erforderlich. Name der Domäne.
-Tablespace -ts	tablespace_name	Erforderlich für eine IBM DB2-Datenbank. Name des Tablespace, in dem sich die Datenbanktabellen für die Domänenkonfiguration befinden.
-SchemaName -sc	schema_name	Optional. Name des Microsoft SQL Server-Schemas. Geben Sie einen Schemanamen ein, wenn Sie nicht das Standardschema verwenden.
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Optional. Gibt an, ob die Informatica-Domänendatenbank mit TLS und SSL sicher ist. Setzen Sie diese Option für die sichere Datenbank auf True. Standardwert ist „False“. Wenn die Option -dbtls ohne Wert angegeben wird, verwendet die Informatica-Domäne die sichere Kommunikation mit der Informatica-Domänendatenbank.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Optional. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.

Option	Argument	Beschreibung
-TrustedConnection -tc	-	Optional. Stellen Sie eine Verbindung zur Microsoft SQL Server-Datenbank über eine vertrauenswürdige Verbindung her. Die vertrauenswürdige Authentifizierung verwendet die Windows-Sicherheitsanmeldedaten des aktuellen Benutzers, um eine Verbindung zu Microsoft SQL Server herzustellen.
-EncryptionKeyLocation -kl	encryption_key_location	Optional. Verzeichnis, das den aktuellen Verschlüsselungsschlüssel enthält. Sie müssen den Schlüsselspeicherort angeben, wenn der Verschlüsselungsschlüssel nicht in der Datei „isp/config/nodemeta.xml“ vorhanden ist. Der Name der Verschlüsselungsdatei lautet „sitekey“.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Pfad und Dateiname der Truststore-Datei für die sichere Domänenrepository-Datenbank. Erforderlich, wenn Sie eine sichere Domänenrepository-Datenbank für die Domäne konfigurieren.

## DefineDomain

Erstellt eine Domäne auf dem aktuellen Computer. Wenn Sie eine Domäne auf einem Computer definieren, auf dem eine Domäne gehostet wird, müssen Sie zuerst die Informatica-Dienste auf dem Computer beenden. Infasetup entfernt die vorhandenen Domänen- und Knoteneinstellungen. Starten Sie nach dem Definieren der neuen Domäne die Informatica-Dienste neu.

Zum Erstellen einer Domäne auf einem Windows-Computer müssen Sie zuerst den Hostport öffnen oder die Firewall deaktivieren.

Geben Sie im Anschluss an die Option (-f) im Befehl DefineDomain keine weiteren Zeichen ein. Wenn Sie zusätzliche Zeichen eingeben, schlägt der Befehl unter Umständen mit einem unerwarteten Fehler fehl.

Der Befehl „DefineDomain“ verwendet die folgende Syntax:

```
DefineDomain
<<-DatabaseAddress|-da> database_hostname:database_port|<-DatabaseConnectionString|-cs>
database_connection_string>
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE|POSTGRESQL
[<-DatabaseServiceName|-ds> database_service_name]
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for MSSQLServer and PostgreSQL only)]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
<-DomainName|-dn> domain_name
[<-DomainDescription|-de> domain_description]
<-AdministratorName|-ad> administrator_name
[<-Password|-pd> password]
[<-LicenseName|-ln> license_name]
[<-LicenseKeyFile|-lf> license_key_file]
<-LogServiceDirectory|-ld> log_service_directory
[<-SystemLogDirectory|-sld> system_log_directory]
<-NodeName|-nn> node_name
<-NodeAddress|-na> node_host:port
[<-ServiceManagerPort|-sp> service_manager_port]
[<-EnableTLS|-tls> enable_tls]
```



```

[<-NodeKeystore|-nk> node_keystore_directory]
[<-NodeKeystorePass|-nkp> node_keystore_password]
[<-NodeTruststore|-nt> node_truststore_directory]
[<-NodeTruststorePass|-ntp> node_truststore_password]
[<-CipherWhiteList|-cwl> comma_separated_white_list_jsse_cipher_names]
[<-CipherBlackList|-cbl> comma_separated_black_list_jsse_cipher_names]
[<-CipherWhiteListFile|-cwlf>
absolute_filename_containing_comma_separated_white_list_jsse_cipher_names]
[<-CipherBlackListFile|-cbf>
absolute_filename_containing_comma_separated_black_list_jsse_cipher_names]
[<-EnableKerberos|-krb> enable_kerberos]
[<-ServiceRealmName|-srn> realm_name_of_node_spn]
[<-UserRealmName|-urn> realm_name_of_user_spn]
[<-KeysDirectory|-kd> Infa_keys_directory_location]
[<-SPNShareLevel|-spnSL> SPNShareLevel PROCESS|NODE]
[<-EnableSaml|-saml> enable_saml]
[<-IdpUrl|-iu> idp_url]
[<-ServiceProviderId|-spid> service_provider_id]
[<-ClockSkewTolerance|-cst> clock_skew_tolerance_in_seconds]
[<-SamlAssertionSigned|-sas> saml_assertion_signed]
[<-AssertionSigningCertificateAlias|-asca> idp_assertion_signing_certificate_alias]
[<-SamlTrustStoreDir|-std> saml_truststore_directory]
[<-SamlTrustStorePassword|-stp> saml_truststore_password]
[<-SamlKeyStoreDir|-skd> saml_keystore_directory]
[<-SamlKeyStorePassword|-skp> saml_keystore_password]
[<-AuthnContextComparsion|-acc> saml_requested_authn_context_comparsion_type]
[<-AuthnContextClassRef|-accr> saml_requested_authn_context_class_reference]
[<-SignSamlRequest|-ssr> sign_saml_request]
[<-RequestSigningPrivateKeyAlias|-rspa> saml_request_signing_private_key_alias]
[<-RequestSigningPrivateKeyPassword|-rspp> saml_request_signing_private_key_password]
[<-RequestSigningAlgorithm|-rsa> saml_request_signing_algorithm]
[<-SamlResponseSigned|-srs> saml_response_signed]
[<-ResponseSigningCertificateAlias|-rsca> idp_response_signing_certificate_alias]
[<-SamlAssertionEncrypted|-sae> saml_assertion_encrypted]
[<-EncryptedAssertionPrivateKeyAlias|-eapa> saml_encrypted_assertion_private_key_alias]
[<-EncryptedAssertionPrivateKeyPassword|-eapp>
saml_encrypted_assertion_private_key_password]
[<-EnablePasswordComplexity|-pc> enable_password_complexity]
[<-AdminconsolePort|-ap> admin_tool_port]
[<-HttpsPort|-hs> admin_tool_https_port]
[<-KeystoreFile|-kf> admin_tool_file_location]
[<-KeystorePass|-kp> admin_tool_keystore_password]
<-MinProcessPort|-mi> minimum_port
<-MaxProcessPort|-ma> maximum_port
[<-ServerPort|-sv> server_shutdown_port]
[<-AdminconsoleShutdownPort|-asp> admin_tool_shutdown_port]
[<-BackupDirectory|-bd> backup_directory]
[<-ServiceResilienceTimeout|-sr> timeout_period_in_seconds]
[<-ErrorLogLevel|-el> FATAL_ERROR_WARNING_INFO_TRACE_DEBUG]
<-ResourceFile|-rf> resource_file
[<-Timezone|-tz> log_service_timezone_GMT+00:00]
[<-Force|-f>]
[<-TrustedConnection|-tc> trusted_connection (used for MSSQLServer only)]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
[<-EnableHsts|-hsts> enable_http_strict_transport_security]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infasetup DefineDomain“ beschrieben:

Option	Beschreibung
-DatabaseAddress -da	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Name und Portnummer des Computers, auf dem die Konfigurationsdatenbank der Domäne gehostet wird.
-DatabaseConnectionString -cs	Erforderlich, wenn Sie die Optionen -DatabaseAddress (-da) und -DatabaseServiceName (-ds) nicht verwenden. Verbindungszeichenfolge, die zum Herstellen einer Verbindung zur Konfigurationsdatenbank der Domäne verwendet wird. Geben Sie den Namen des Datenbankhosts, -ports und -diensts als Teil der Verbindungszeichenfolge ein. Setzen Sie die Verbindungszeichenfolge in Anführungszeichen.
-DatabaseUserName -du	Erforderlich, wenn Sie die Option -TrustedConnection (-tc) nicht verwenden. Konto für die Datenbank, die die Domänenkonfigurationsinformationen enthält.
-DatabasePassword -dp	Passwort aus der Datenbank für die Domänenkonfiguration des Datenbankbenutzers. Wenn Sie diese Option weglassen, verwendet <i>infasetup</i> das in der Umgebungsvariable <code>INFA_DEFAULT_DATABASE_PASSWORD</code> angegebene Passwort. Wenn in der Umgebungsvariable kein Wert angegeben ist, müssen Sie mithilfe dieser Option ein Passwort eingeben.
-DatabaseType -dt	Erforderlich. Typ der Datenbank, in der die Domänenkonfigurationsmetadaten gespeichert werden. Zu den Datenbanktypen gehören: <ul style="list-style-type: none"> <li>- db2</li> <li>- oracle</li> <li>- mssqlserver</li> <li>- sybase</li> <li>- postgresql</li> </ul>
-DatabaseServiceName -ds	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Der Name des Datenbankdiensts. Erforderlich für Oracle-, IBM DB2- und Microsoft SQL Server-Datenbanken. Geben Sie die SID für Oracle, den Dienstnamen für IBM DB2 oder den Datenbanknamen für Microsoft SQL Server ein.
-Tablespace -ts	Erforderlich für eine IBM DB2-Datenbank. Name des Tablespace, in dem sich die Datenbanktabellen für die Domänenkonfiguration befinden.
-SchemaName -sc	Optional. Name des Microsoft SQL Server- oder des PostgreSQL-Schemas. Geben Sie einen Schemanamen ein, wenn Sie nicht das Standardschema verwenden.
-DatabaseTlsEnabled -dbtls	Optional. Gibt an, ob die Informatica-Domänendatenbank mit TLS und SSL sicher ist. Setzen Sie diese Option für die sichere Datenbank auf True. Standardwert ist „False“. Wenn die Option -dbtls ohne Wert angegeben wird, verwendet die Informatica-Domäne die sichere Kommunikation mit der Informatica-Domänendatenbank.
-DatabaseTruststorePassword -dbtp	Optional. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.

Option	Beschreibung
-DomainName -dn	Erforderlich. Name der Domäne. Domännennamen müssen zwischen 1 und 79 Zeichen umfassen und dürfen weder Leerzeichen noch die folgenden Zeichen enthalten: / * ? < > "
-DomainDescription -de	Optional. Beschreibung der Domäne.
-AdministratorName -ad	Erforderlich. Benutzername des Domänenadministrators. Wenn die Domäne einen einzelnen Kerberos-Bereich zum Authentifizieren von Benutzern verwendet, geben Sie den SAM-Kontonamen an. Wenn die Domäne die bereichsübergreifende Kerberos-Authentifizierung verwendet, geben Sie den vollqualifizierten Benutzerprinzipalnamen, einschließlich des Bereichsnamens, an. Beispiel: sysadmin@COMPANY.COM
-Password -pd	Optional für Kerberos-Domäne. Passwort des Domänenadministrators. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang. Wenn Sie für ein natives Benutzerkonto die Passwortkomplexität aktivieren, beachten Sie beim Erstellen oder Ändern eines Passworts Folgendes: - Das Passwort muss aus mindestens acht Zeichen bestehen. - Es muss mindestens einen Buchstaben, eine Zahl und ein nicht alphanumerisches Zeichen enthalten, z. B.: ! \ " # \$ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` {   } ~ Manche Sonderzeichen in Passwörtern können von der Shell anders interpretiert werden. Beispielsweise wird \$ als Variable interpretiert. Setzen Sie in diesem Fall ein Escape-Zeichen vor das betreffende Sonderzeichen.
-LicenseName -ln	Optional. Name der Lizenz. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten: / * ? < > "
-LicenseKeyFile -lf	Optional. Pfad zur Lizenzschlüsseldatei.
-LogServiceDirectory -ld	Erforderlich. Freigegebener Verzeichnispfad, der vom Protokollmanager zum Speichern von Protokollereignisdateien verwendet wird. Stellen Sie sicher, dass -ld nicht übereinstimmt oder den angegebenen Wert für -sld enthält.
-SystemLogDirectory -sld	Optional. Verzeichnispfad zum Speichern von Systemprotokolldateien. Stellen Sie sicher, dass -ld nicht übereinstimmt oder den angegebenen Wert für -sld enthält. Standard ist <INFA_home>/logs.
-NodeName -nn	Erforderlich. Name des Knotens. Knotennamen müssen zwischen 1 und 79 Zeichen umfassen und dürfen weder Leerzeichen noch die folgenden Zeichen enthalten: \ / * ? < > "
-NodeAddress -na	Erforderlich. Hostname und Portnummer für den Computer, auf dem der Knoten gehostet wird. Wählen Sie eine verfügbare Portnummer aus.

Option	Beschreibung
-ServiceManagerPort -sp	Optional. Portnummer, die vom Dienstmanager verwendet wird, um auf eingehende Verbindungsanfragen zu reagieren.
-EnableTLS -tls	<p>Optional. Konfiguriert die sichere Kommunikation für die Dienste in der Informatica-Domäne.</p> <p>Wenn Sie die standardmäßigen, von Informatica bereitgestellten SSL-Zertifikate verwenden, müssen Sie die Schlüsselspeicher- und Truststore-Optionen nicht angeben. Wenn Sie das SSL-Zertifikat nicht verwenden, müssen Sie die Keystore- und Truststore-Optionen angeben. Gültige Werte sind „True“ oder „False“. Standardwert ist „False“. Wenn Sie die Option -tls ohne Wert angeben, verwendet die Informatica-Domäne die sichere Kommunikation zwischen Diensten.</p> <p>Zum Aktivieren der sicheren Kommunikation für die verbundenen Dienste oder Webanwendungen, z. B. das Administrator Tool, das Analyst Tool oder den Webdienst-Hub, konfigurieren Sie die sichere Kommunikation separat innerhalb der Anwendungen.</p>
-NodeKeystore- -nk	<p>Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Verzeichnis, das die Schlüsselspeicherdateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS-Dateien (Java Keystore) vorliegen. Das Verzeichnis muss Schlüsselspeicherdateien in den Formaten PEM und JKS enthalten.</p> <p>Die Schlüsselspeicherdateien müssen infa_keystore.jks und infa_keystore.pem lauten. Wenn die Schlüsselspeicherdatei, die Sie von der Zertifizierungsstelle erhalten, einen anderen Namen hat, müssen Sie sie in infa_keystore.jks und infa_keystore.pem umbenennen.</p> <p>Sie müssen für alle Knoten in der Domäne dieselben Schlüsselspeicherzertifikate verwenden.</p>
-NodeKeystorePass -nkp	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die Schlüsselspeicherdatei infa_keystore.jks.
-NodeTruststore -nt	<p>Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Verzeichnis, das die Truststore-Dateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS-Dateien (Java Keystore) vorliegen. Das Verzeichnis muss Truststore-Dateien in den Formaten PEM und JKS enthalten.</p> <p>Die Truststore-Dateien müssen die Namen infa_truststore.jks und infa_truststore.pem aufweisen. Wenn die Truststore-Datei, die Sie von der Zertifizierungsstelle erhalten haben, einen anderen Namen aufweist, müssen Sie sie in infa_truststore.jks und infa_truststore.pem umbenennen.</p>
-NodeTruststorePass -ntp	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die Datei infa_truststore.jks.
-CipherWhiteList -cwl	<p>Optional. Eine kommagetrennte Liste mit JSSE-Chiffre-Suites, die zur Gültigkeitsliste hinzugefügt werden sollen.</p> <p><b>Hinweis:</b> Die Liste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.</p>

Option	Beschreibung
-CipherBlackList -cbl	Optional. Eine kommasetrennte Liste mit JSSE-Chiffre-Suites, die aus der Gültigkeitsliste entfernt werden sollen. <b>Hinweis:</b> Die Gültigkeitsliste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-CipherWhiteListFile -cwlf	Optional. Absoluter Dateiname der Klartextdatei, die eine kommasetrennte Liste mit Chiffre-Suites enthält, die der Gültigkeitsliste hinzugefügt werden sollen. <b>Hinweis:</b> Die Liste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-CipherBlackListFile -cblf	Optional. Absoluter Dateiname der Klartextdatei, die eine kommasetrennte Liste mit Chiffre-Suites enthält, die aus der Gültigkeitsliste entfernt werden sollen. <b>Hinweis:</b> Die Gültigkeitsliste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-EnableKerberos -krb	Optional. Konfiguriert die Informatica-Domäne zur Verwendung der Kerberos-Authentifizierung. Gültige Werte sind „True“ oder „False“. Bei True verwendet die Domäne die Kerberos-Authentifizierung, dann können Sie den Authentifizierungsmodus später nicht ändern. Nachdem Sie die Kerberos-Authentifizierung aktiviert haben, können Sie sie nicht deaktivieren. Der Standardwert ist „false“. Wenn Sie die Option -krb ohne einen Wert angeben, verwendet die Informatica-Domäne die Kerberos-Authentifizierung.
-ServiceRealmName -srn	Optional. Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung. Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie die Namen aller Kerberos-Bereiche, die von der Domäne zum Authentifizieren von Benutzern verwendet werden, getrennt durch Kommas ein. Beispiel: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Geben Sie beispielsweise folgenden Wert an, um alle Bereiche einzuschließen, die den Namen EAST.COMPANY.COM enthalten: *EAST.COMPANY.COM
-UserRealmName -urn	Optional. Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung. Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie die Namen aller Kerberos-Bereiche, die von der Domäne zum Authentifizieren von Benutzern verwendet werden, getrennt durch Kommas ein. Beispiel: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Geben Sie beispielsweise folgenden Wert an, um alle Bereiche einzuschließen, die den Namen EAST.COMPANY.COM enthalten: *EAST.COMPANY.COM

Option	Beschreibung
-KeysDirectory -kd	Optional. Verzeichnis, in dem alle Schlüsseltabellendateien und der Verschlüsselungsschlüssel für die Informatica-Domäne gespeichert werden. Standardwert ist <code>&lt;Informatica installation directory&gt;/isp/config/keys</code> .
-SPNShareLevel -spnSL	Optional. Gibt die Dienst-Prinzipalebene für die Domäne an. Legen Sie eine der folgenden Ebenen für die Eigenschaft fest: <ul style="list-style-type: none"> <li>- Prozess Die Domäne erfordert einen eindeutigen Dienst-Prinzipalnamen (SPN) und eine Keytab-Datei für jeden Knoten und für jeden Dienst auf einem Knoten. Die Anzahl der pro Knoten erforderlichen SPNs und Keytab-Dateien hängt von der Anzahl der Dienstprozesse ab, die auf dem Knoten ausgeführt werden. Verwenden Sie die Knotenebenen-Option, wenn die Domäne keine hohe Sicherheitsstufe erfordert.</li> <li>- Knoten. Die Domäne verwendet einen SPN und eine Keytab-Datei für den Knoten und für alle Dienste, die auf dem Knoten ausgeführt werden. Sie erfordert außerdem einen separaten SPN und eine separate Keytab-Datei für alle HTTP-Prozesse auf dem Knoten.</li> </ul> Standardwert ist „Prozess“.
-EnableSaml -saml	Optional. Aktiviert oder deaktiviert die SAML-Authentifizierung in der Informatica-Domäne.  Legen Sie diesen Wert auf „true“ fest, um die SAML-Authentifizierung in der Informatica-Domäne zu aktivieren. Der Standardwert ist „false“.
-idpUrl -iu	Erforderlich, wenn die Option -saml auf TRUE festgelegt ist. Geben Sie die URL des SAML-Identitätsanbieters an.
-ServiceProviderId -spid	Optional. Der Vertrauensstellungsname der vertrauenswürdigen Partei oder die Kennung des Dienstanbieters für die Domäne, wie im Identitätsanbieter definiert.  Wenn Sie „Informatica“ als Vertrauensstellungsname der vertrauenswürdigen Partei in AD FS angegeben haben, müssen Sie keinen Wert angeben.
-ClockSkewTolerance -cst	Optional. Der zulässige zeitliche Unterschied zwischen der Systemuhr des Identitätsanbieter-Hosts und der Systemuhr auf dem Master-Gateway-Knoten.  Die Lebensdauer von SAML-Token, die vom Identitätsanbieter ausgegeben werden, wird entsprechend der Systemuhr des Identitätsanbieter-Hosts festgelegt. Die Lebensdauer eines von Identitätsanbieter ausgegebenen SAML-Tokens ist gültig, wenn die im Token festgelegte Startzeit oder Endzeit nicht mehr als die angegebene Anzahl an Sekunden von der Systemuhr auf dem Master-Gateway-Knoten abweicht.  Die Werte müssen zwischen 0 und 600 Sekunden liegen. Standardwert ist 120 Sekunden.
-SamlAssertionSigned -sas	Optional. Setzen Sie den Parameter auf TRUE, um das Signieren von Assertionen durch den Identitätsanbieter zu aktivieren. Standardwert ist FALSE.
-AssertionSigningCertificateAlias -asca	Erforderlich, wenn SamlAssertionSigned auf TRUE gesetzt ist. Der Aliasname, der beim Importieren des Assertionssignaturzertifikats des Identitätsanbieters in die für die SAML-Authentifizierung verwendete Truststore-Datei angegeben wird.

Option	Beschreibung
-SamlTrustStoreDir -std	Optional. Das Verzeichnis mit der benutzerdefinierten Truststore-Datei, die zur Verwendung von SAML-Authentifizierung auf Gateway-Knoten innerhalb der Domäne erforderlich ist. Geben Sie nur das Verzeichnis an, nicht den vollständigen Pfad zur Datei. Der Informatica-Standard-Truststore wird verwendet, wenn kein Truststore angegeben ist.
-SamlTrustStorePassword -stp	Erforderlich, wenn Sie einen benutzerdefinierten Truststore für die SAML-Authentifizierung verwenden. Das Passwort für die benutzerdefinierte Truststore-Datei.
-SamlKeyStoreDir -skd	Optional. Das Verzeichnis mit der benutzerdefinierten Schlüsselspeicher-Datei, die für die Verwendung der SAML-Authentifizierung auf dem Gateway-Knoten erforderlich ist. Geben Sie nur das Verzeichnis an, nicht den vollständigen Pfad zur Datei.
-SamlKeyStorePassword -skp	Erforderlich, wenn Sie einen benutzerdefinierten Schlüsselspeicher für die SAML-Authentifizierung verwenden. Passwort für den SAML-Schlüsselspeicher. *
-AuthnContextComparsion -acc	Gibt die Vergleichsmethode an, mit der die angeforderte Berechtigungserklärung ausgewertet wird. Eine der folgenden Optionen: <ul style="list-style-type: none"> <li>- MINIMUM. Der Authentifizierungskontext in der Authentifizierungsanweisung muss genau mit mindestens einem der angegebenen Authentifizierungskontexte übereinstimmen.</li> <li>- MAXIMUM. Der Authentifizierungskontext in der Authentifizierungsanweisung muss mindestens so stark (wie vom Antwortenden angenommen) sein wie einer der angegebenen Authentifizierungskontexte.</li> <li>- BETTER. Der Authentifizierungskontext in der Authentifizierungsanweisung muss stärker (wie vom Antwortenden angenommen) sein wie einer der angegebenen Authentifizierungskontexte.</li> <li>- EXACT. Der Authentifizierungskontext in der Authentifizierungsanweisung muss so stark wie möglich (wie vom Antwortenden angenommen) sein, ohne die Stärke von mindestens einem der angegebenen Authentifizierungskontexte zu überschreiten.</li> </ul> Der Standardwert ist EXACT.
-AuthnContextClassRef -accr	Die Klasse des Authentifizierungskontexts. Eine der folgenden Optionen: <ul style="list-style-type: none"> <li>- PASSWORD</li> <li>- PASSWORDPROTECTEDTRANSPORT</li> </ul>
-SignSamlRequest -ssr	Setzen Sie den Parameter auf „True“, um die Signieranforderung zu aktivieren. Standardwert ist „False“.
-RequestSigningPrivateKeyAlias -rspa	Erforderlich, wenn Sie die Signieranforderung aktivieren. Aliasname des privaten Schlüssels im SAML-Schlüsselspeicher des Knotens, mit dem die SAML-Anforderung signiert werden soll.
-RequestSigningPrivateKeyPassword -rspp	Erforderlich, wenn Sie die Signieranforderung aktivieren. Passwort für den Zugriff auf den privaten Schlüssel, der zum Signieren der SAML-Anforderung verwendet wird.

Option	Beschreibung
-RequestSigningAlgorithm -rsa	Erforderlich, wenn Sie die Signieranforderung aktivieren. Algorithmus zum Signieren der Anforderung. Eine der folgenden Optionen: <ul style="list-style-type: none"> <li>- RSA_SHA256</li> <li>- DSA_SHA1</li> <li>- DSA_SHA256</li> <li>- RSA_SHA1</li> <li>- RSA_SHA224</li> <li>- RSA_SHA384</li> <li>- RSA_SHA512</li> <li>- ECDSA_SHA1</li> <li>- ECDSA_SHA224</li> <li>- ECDSA_SHA256</li> <li>- ECDSA_SHA384</li> <li>- ECDSA_SHA512</li> <li>- RIPEMD160</li> <li>- RSA_MD5</li> </ul>
-SamlResponseSigned -srs	Setzen Sie den Parameter auf „True“, um die signierte Antwort zu aktivieren. Der Standardwert ist FALSE.
-ResponseSigningCertificateAlias -rsca	Erforderlich, wenn Sie die signierte Antwort aktivieren. Aliasname des Zertifikats im SAML-Truststore des Gateway-Knotens, mit dem die SAML-Antwortsignatur überprüft wird.
-SamlAssertionEncrypted -sae	Erforderlich, wenn Sie die signierte Antwort aktivieren. Setzen Sie den Parameter auf „True“, um die verschlüsselte Assertion zu aktivieren. Der Standardwert ist FALSE.
-EncryptedAssertionPrivateKeyAlias -espa	Erforderlich, wenn Sie die verschlüsselte Assertion aktivieren. Aliasname des privaten Schlüssels im SAML-Schlüsselspeicher des Gateway-Knotens, mit dem der Schlüssel zum Verschlüsseln der Assertion entschlüsselt wird.
-EncryptedAssertionPrivateKeyPassword -espp	Erforderlich, wenn Sie die verschlüsselte Assertion aktivieren. Passwort für den Zugriff auf den privaten Schlüssel an, der zum Entschlüsseln des Assertion-Verschlüsselungsschlüssels verwendet wird.
-EnablePasswordComplexity -pc	Optional. Aktiviert die Passwortkomplexität, um die Passwortstärke zu validieren.  Wenn Sie für ein natives Benutzerkonto die Passwortkomplexität aktivieren, beachten Sie beim Erstellen oder Ändern eines Passworts Folgendes: <ul style="list-style-type: none"> <li>- Das Passwort muss aus mindestens acht Zeichen bestehen.</li> <li>- Es muss mindestens einen Buchstaben, eine Zahl und ein nicht alphanumerisches Zeichen enthalten, z. B.:  ! \ " # \$ % &amp; ' ( ) * + , - . / : ; &lt; = &gt; ? @ [ ] ^ _ ` {   } ~ </li> </ul> Manche Sonderzeichen in Passwörtern können von der Shell anders interpretiert werden. Beispielsweise wird \$ als Variable interpretiert. Setzen Sie in diesem Fall ein Escape-Zeichen vor das betreffende Sonderzeichen.
-AdminconsolePort -ap	Port für den Zugriff auf Informatica Administrator.
-HttpsPort -hs	Optional. Portnummer zum Sichern der Verbindung zum Administrator Tool. Geben Sie diese Portnummer an, wenn Sie HTTPS für einen Knoten konfigurieren möchten.



Option	Beschreibung
-KeystoreFile -kf	Optional. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die bei Verwendung des SSL-Protokolls erforderlich sind
-KeystorePass -kp	Optional. Ein Klartext-Passwort für die Schlüsselspeicherdatei. Sie können ein Passwort mit der Option -kp oder der Umgebungsvariable INFA_PASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -kp festgelegte Passwort Vorrang.
-MinProcessPort -mi	Erforderlich. Kleinste Portnummer für die Anwendungsdienstprozesse, die auf dem Knoten ausgeführt werden.
-MaxProcessPort -ma	Erforderlich. Größte Portnummer für die Anwendungsdienstprozesse, die auf dem Knoten ausgeführt werden.
-ServerPort -sv	Optional. Vom Dienstmanager verwendete TCP/IP-Portnummer. Der Dienstmanager verwaltet Befehle zum Herunterfahren aus Domänenkomponenten auf diesem Port. Legen Sie diese Portnummer fest, wenn sich auf einem Computer mehrere Knoten befinden oder die Standardportnummer verwendet wird. Als Standardwert fungiert die Portnummer des Knotens plus eins.
-AdminconsoleShutdownPort -asp	Portnummer, die das Herunterfahren für Informatica Administrator steuert.
-BackupDirectory -bd	Optional. Verzeichnis zum Speichern der Repository-Backup-Dateien. Der Zugriff auf das Verzeichnis muss über den Knoten möglich sein.
-ServiceResilienceTimeout -sr	Optional. Zeit in Sekunden, in der <i>infasetup</i> versucht, eine Verbindung zur lokalen Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet <i>infasetup</i> den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben ist, wird der Standardwert von 180 Sekunden verwendet.
-ErrorLogLevel -el	Optional. Schweregradstufe für Protokollereignisse im Domänenprotokoll. Standardwert ist „info“.
-ResourceFile -rf	Erforderlich. Datei, die eine Liste der verfügbaren Ressourcen für den Knoten enthält. Verwenden Sie die Datei „nodeoptions.xml“, die sich an folgendem Speicherort befindet: <Informatica installation directory>/isp/bin
-TimeZone -tz	Optional. Zeitzone, die vom Protokollmanager beim Erzeugen von Protokollereignisdateien verwendet wird. Standardwert ist GMT+00:00. Konfigurieren Sie die Zeitzone in folgendem Format:  GMT (+/-) hh:mm
-Force -f	Optional. Überschreibt die Datenbank, wenn eine Datenbank mit demselben Namen bereits vorhanden ist. Geben Sie im Anschluss an diese Option keine weiteren Zeichen ein.

Option	Beschreibung
-TrustedConnection -tc	Optional. Stellen Sie eine Verbindung zur Microsoft SQL Server-Datenbank über eine vertrauenswürdige Verbindung her. Die vertrauenswürdige Authentifizierung verwendet die Windows-Sicherheitsanmeldedaten des aktuellen Benutzers, um eine Verbindung zu Microsoft SQL Server herzustellen. <b>Hinweis:</b> Wenn Sie eine vertrauenswürdige Verbindung verwenden, konfigurieren Sie die Option DatabaseConnectionString.
-DatabaseTruststoreLocation -dbtl	Pfad und Dateiname der Truststore-Datei für die sichere Domänenrepository-Datenbank. Erforderlich, wenn Sie eine sichere Domänenrepository-Datenbank für die Domäne konfigurieren.
EnableHsts -hsts	Optional. Setzen Sie diesen Parameter auf TRUE, um HTTP Strict Transport Security zu aktivieren. Für HTTP Strict Transport Security müssen Webanwendungen HTTPS verwenden.
* Hinweis: Wenn Sie derzeit Skripts ausführen, die diesen Befehl verwenden, um einen benutzerdefinierten Schlüsselspeicher für die SAML-Authentifizierung zu aktivieren, müssen Sie diese aktualisieren, um diese Option aufzunehmen.	

Wenn Sie DefineDomain auf einem Knoten ausführen, auf dem aktuell eine Domäne gehostet wird, konfigurieren Sie die folgenden Domäneneigenschaften neu:

- **Anwendungsdienste.** Erstellen Sie einen beliebigen Anwendungsdienst neu, der in der Domäne ausgeführt wurde.
- **Benutzer.** Erstellen Sie Benutzer neu.
- **Gateway-Knoten.** Konfigurieren Sie Gateway-Knoten in der Domäne.
- **Allgemeine Domäneneigenschaften.** Konfigurieren Sie Belastbarkeits-Timeout und die maximale Anzahl von Neustartversuchen für die Domäne.
- **Gitter.** Erstellen Sie ein beliebiges Gitter in der Domäne neu.
- **LDAP-Authentifizierung.** Konfigurieren Sie LDAP-Authentifizierung für die Domäne.
- **Log Manager-Eigenschaften.** Konfigurieren Sie den freigegebenen Verzeichnispfad, die Bereinigen-Eigenschaften und die Zeitzone des Log Managers.

Wenn Sie den Hostnamen oder die Portnummer des Gateway-Knotens ändern, müssen Sie darüber hinaus jeden Knoten unter Verwendung des *infacmd* AddDomainNode-Befehls zur Domäne hinzufügen.

## DefineGatewayNode

Definiert einen Gateway-Knoten auf dem aktuellen Computer. Dieser Befehl überschreibt die Datei nodemeta.xml, welche die Konfigurationsmetadaten für den Knoten speichert. Nachdem Sie den Knoten definiert haben, führen Sie den Befehl *infacmd* isp AddDomainNode aus, um den Knoten zur Domäne hinzuzufügen.

Der Befehl „DefineGatewayNode“ verwendet die folgende Syntax:

```
DefineGatewayNode
<-DatabaseAddress|-da> database_hostname:database_port|<-DatabaseConnectionString|-cs>
database_connection_string>
```

```

[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE|POSTGRESQL
[<-DatabaseServiceName|-ds> database_service_name]
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
<-NodeAddress|-na> node_host:port
[<-ServiceManagerPort|-sp> service_manager_port]
[<-EnableTLS|-tls> enable_tls]
[<-NodeKeystore|-nk> node_keystore_directory]
[<-NodeKeystorePass|-nkp> node_keystore_password]
[<-NodeTruststore|-nt> node_truststore_directory]
[<-NodeTruststorePass|-ntp> node_truststore_password]
[<-CipherWhiteList|-cwl> comma_separated_white_list_jsse_cipher_names]
[<-CipherBlackList|-cbl> comma_separated_black_list_jsse_cipher_names]
[<-CipherWhiteListFile|-cwlf>
absolute_filename_containing_comma_separated_white_list_jsse_cipher_names]
[<-CipherBlackListFile|-cblf>
absolute_filename_containing_comma_separated_black_list_jsse_cipher_names]
[<-EnableKerberos|-krb> enable_kerberos]
[<-ServiceRealmName|-srn> realm_name_of_node_spn]
[<-UserRealmName|-urn> realm_name_of_user_spn]
[<-KeysDirectory|-kd> infra_keys_directory_location]
[<-EnableSaml|-saml> enable_saml]
[<-SamlTrustStoreDir|-std> saml_truststore_directory]
[<-SamlTrustStorePassword|-stp> saml_truststore_password]
[<-SamlKeyStoreDir|-skd> saml_keystore_directory]
[<-SamlKeyStorePassword|-skp> saml_keystore_password]
[<-AdminconsolePort|-ap> admin_tool_port]
[<-HttpsPort|-hs> admin_tool_https_port]
[<-KeystoreFile|-kf> admin_tool_keystore_file_location]
[<-KeystorePass|-kp> admin_tool_keystore_password]
[<-MinProcessPort|-mi> minimum_port]
[<-MaxProcessPort|-ma> maximum_port]
<-LogServiceDirectory|-ld> log_service_directory
[<-SystemLogDirectory|-sld> system_log_directory]
[<-ServerPort|-sv> server_shutdown_port]
[<-AdminconsoleShutdownPort|-asp> admin_tool_shutdown_port]
[<-BackupDirectory|-bd> backup_directory]
[<-ErrorLogLevel|-el> FATAL_ERROR_WARNING_INFO_TRACE_DEBUG]
<-ResourceFile|-rf> resource_file
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for MSSQLServer and PostgreSQL only)]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-TrustedConnection|-tc> trusted_connection (used for MSSQLServer only)]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]

```

In der folgenden Tabelle werden die Optionen und Argumente für „*infasetup DefineGatewayNode*“ beschrieben:

Option	Beschreibung
-DatabaseAddress -da	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Name und Portnummer des Computers, auf dem die Konfigurationsdatenbank der Domäne gehostet wird.
-DatabaseConnectionString -cs	Erforderlich, wenn Sie die Optionen -DatabaseAddress (-da) und -DatabaseServiceName (-ds) nicht verwenden. Verbindungszeichenfolge, die zum Herstellen einer Verbindung zur Konfigurationsdatenbank der Domäne verwendet wird. Geben Sie den Namen des Datenbankhosts, -ports und -diensts als Teil der Verbindungszeichenfolge ein. Setzen Sie die Verbindungszeichenfolge in Anführungszeichen.

Option	Beschreibung
-DatabaseUserName -du	Erforderlich, wenn Sie die Option -TrustedConnection (-tc) nicht verwenden. Konto für die Datenbank, die die Domänenkonfigurationsinformationen enthält.
-DatabasePassword -dp	Passwort aus der Datenbank für die Domänenkonfiguration des Datenbankbenutzers. Wenn Sie diese Option weglassen, verwendet <i>infasetup</i> das in der Umgebungsvariable <code>INFA_DEFAULT_DATABASE_PASSWORD</code> angegebene Passwort. Wird in der Umgebungsvariable kein Wert angegeben, müssen Sie ein Passwort unter Verwendung dieser Option eingeben.
-DatabaseType -dt	Erforderlich. Typ der Datenbank, in der die Domänenkonfigurationsmetadaten gespeichert werden. Zu den Datenbanktypen gehören: <ul style="list-style-type: none"> <li>- db2</li> <li>- oracle</li> <li>- mssqlserver</li> <li>- sybase</li> <li>- postgresql</li> </ul>
-DatabaseServiceName -ds	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Der Name des Datenbankdiensts. Erforderlich für Oracle-, IBM DB2- und Microsoft SQL Server-Datenbanken. Geben Sie die SID für Oracle, den Dienstnamen für IBM DB2 oder den Datenbanknamen für Microsoft SQL Server ein.
-DomainName -dn	Erforderlich. Name der Domäne.
-NodeName -nn	Optional. Name des Knotens. Knotennamen müssen zwischen 1 und 79 Zeichen umfassen und dürfen weder Leerzeichen noch die folgenden Zeichen enthalten: \ / * ? < > "
-NodeAddress -na	Optional. Hostname und Portnummer für den Computer, auf dem der Knoten gehostet wird. Wählen Sie eine verfügbare Portnummer aus.
-ServiceManagerPort -sp	Optional. Portnummer, die vom Dienstmanager verwendet wird, um auf eingehende Verbindungsanfragen zu reagieren.
-EnableTLS -tls	Optional. Konfiguriert die sichere Kommunikation für die Dienste in der Informatica-Domäne.  Wenn Sie die standardmäßigen, von Informatica bereitgestellten SSL-Zertifikate verwenden, müssen Sie die Schlüsselspeicher- und Truststore-Optionen nicht angeben. Wenn Sie das SSL-Zertifikat nicht verwenden, müssen Sie die Keystore- und Truststore-Optionen angeben. Gültige Werte sind „True“ oder „False“. Standardwert ist „False“. Wenn Sie die Option -tls ohne Wert angeben, verwendet die Informatica-Domäne die sichere Kommunikation zwischen Diensten.  Zum Aktivieren der sicheren Kommunikation für die verbundenen Dienste oder Webanwendungen, z. B. das Administrator Tool, das Analyst Tool oder den Webdienst-Hub, konfigurieren Sie die sichere Kommunikation separat innerhalb der Anwendungen.

Option	Beschreibung
-NodeKeystore -nk	<p>Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Verzeichnis, das die Schlüsselspeicherdateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS-Dateien (Java Keystore) vorliegen. Das Verzeichnis muss Schlüsselspeicherdateien in den Formaten PEM und JKS enthalten.</p> <p>Die Schlüsselspeicherdateien müssen infa_keystore.jks und infa_keystore.pem lauten. Wenn die Schlüsselspeicherdatei, die Sie von der Zertifizierungsstelle erhalten, einen anderen Namen hat, müssen Sie sie in infa_keystore.jks und infa_keystore.pem umbenennen.</p> <p>Sie müssen für alle Knoten in der Domäne dieselben Schlüsselspeicherzertifikate verwenden.</p>
-NodeKeystorePass -nkp	<p>Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die Schlüsselspeicherdatei infa_keystore.jks.</p>
-NodeTruststore -nt	<p>Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Verzeichnis, das die Truststore-Dateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS-Dateien (Java Keystore) vorliegen. Das Verzeichnis muss Truststore-Dateien in den Formaten PEM und JKS enthalten.</p> <p>Die Truststore-Dateien müssen die Namen infa_truststore.jks und infa_truststore.pem aufweisen. Wenn die Truststore-Datei, die Sie von der Zertifizierungsstelle erhalten haben, einen anderen Namen aufweist, müssen Sie sie in infa_truststore.jks und infa_truststore.pem umbenennen.</p>
-NodeTruststorePass -ntp	<p>Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die Datei infa_truststore.jks.</p>
-CipherWhiteList -cwl	<p>Optional. Eine kommagetrennte Liste mit JSSE-Chiffre-Suites, die zur Gültigkeitsliste hinzugefügt werden sollen.</p> <p><b>Hinweis:</b> Die Liste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.</p>
-CipherBlackList -cbl	<p>Optional. Eine kommagetrennte Liste mit JSSE-Chiffre-Suites, die aus der Gültigkeitsliste entfernt werden sollen.</p> <p><b>Hinweis:</b> Die Gültigkeitsliste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.</p>
-CipherWhiteListFile -cwlf	<p>Optional. Absoluter Dateiname der Klartextdatei, die eine kommagetrennte Liste mit Chiffre-Suites enthält, die der Gültigkeitsliste hinzugefügt werden sollen.</p> <p><b>Hinweis:</b> Die Liste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.</p>
-CipherBlackListFile -cblf	<p>Optional. Absoluter Dateiname der Klartextdatei, die eine kommagetrennte Liste mit Chiffre-Suites enthält, die aus der Gültigkeitsliste entfernt werden sollen.</p> <p><b>Hinweis:</b> Die Gültigkeitsliste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.</p>

Option	Beschreibung
-EnableKerberos -krb	Optional. Konfiguriert die Informatica-Domäne zur Verwendung der Kerberos-Authentifizierung. Gültige Werte sind „True“ oder „False“. Bei True verwendet die Domäne die Kerberos-Authentifizierung, dann können Sie den Authentifizierungsmodus später nicht ändern. Nachdem Sie die Kerberos-Authentifizierung aktiviert haben, können Sie sie nicht deaktivieren. Standardwert ist „False“. Wenn Sie die Option -krb ohne einen Wert angeben, verwendet die Informatica-Domäne die Kerberos-Authentifizierung.
-ServiceRealmName -srn	Optional. Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung.  Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie die Namen aller Kerberos-Bereiche, die von der Domäne zum Authentifizieren von Benutzern verwendet werden, getrennt durch Kommas ein. Beispiel: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM  Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Geben Sie beispielsweise folgenden Wert an, um alle Bereiche einzuschließen, die den Namen EAST.COMPANY.COM enthalten: *EAST.COMPANY.COM
-UserRealmName -urn	Optional. Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung.  Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie die Namen aller Kerberos-Bereiche, die von der Domäne zum Authentifizieren von Benutzern verwendet werden, getrennt durch Kommas ein. Beispiel: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM  Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Geben Sie beispielsweise folgenden Wert an, um alle Bereiche einzuschließen, die den Namen EAST.COMPANY.COM enthalten: *EAST.COMPANY.COM
-KeysDirectory -kd	Optional. Verzeichnis, in dem alle Schlüsseltabellendateien und der Verschlüsselungsschlüssel für die Informatica-Domäne gespeichert werden. Standardwert ist <Informatica-Installationsverzeichnis>/isp/config/keys.
-EnableSaml -saml	Optional. Aktiviert oder deaktiviert die SAML-Authentifizierung in der Informatica-Domäne.  Legen Sie diesen Wert auf „true“ fest, um die SAML-Authentifizierung in der Informatica-Domäne zu aktivieren. Der Standardwert ist „false“.
-SamlTrustStoreDir -std	Optional. Das Verzeichnis mit der benutzerdefinierten Truststore-Datei, die für die Verwendung der SAML-Authentifizierung auf dem Gateway-Knoten erforderlich ist. Geben Sie nur das Verzeichnis an, nicht den vollständigen Pfad zur Datei.  Der Informatica-Standard-Truststore wird verwendet, wenn kein Truststore angegeben ist.

Option	Beschreibung
-SamlTrustStorePassword -stp	Erforderlich, wenn Sie einen benutzerdefinierten Truststore für die SAML-Authentifizierung verwenden. Das Passwort für den benutzerdefinierten Truststore.
-SamlKeyStoreDir -skd	Optional. Das Verzeichnis mit der benutzerdefinierten Truststore-Datei, die für die Verwendung der SAML-Authentifizierung auf dem Gateway-Knoten erforderlich ist. Geben Sie nur das Verzeichnis an, nicht den vollständigen Pfad zur Datei.
-SamlKeyStorePassword -skp	Erforderlich, wenn Sie einen benutzerdefinierten Schlüsselspeicher für die SAML-Authentifizierung verwenden. Passwort für den SAML-Schlüsselspeicher. *
-AdminconsolePort -ap	Optional. Port für den Zugriff auf Informatica Administrator.
-HttpsPort -hs	Optional. Portnummer, die vom Knoten für die Kommunikation zwischen dem Administrator Tool und dem Dienstmanager verwendet wird. Geben Sie diese Portnummer an, wenn Sie HTTPS für einen Knoten konfigurieren möchten.  Zum Deaktivieren von HTTPS-Unterstützung für einen Knoten setzen Sie diese Portnummer auf Null.
-KeystoreFile -kf	Optional. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die bei Verwendung des SSL-Protokolls erforderlich sind
-KeystorePass -kp	Optional. Ein Klartext-Passwort für die Schlüsselspeicherdatei. Sie können ein Passwort mit der Option -kp oder der Umgebungsvariable INFA_PASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -kp festgelegte Passwort Vorrang.
-MinProcessPort -mi	Optional. Kleinste Portnummer für die Anwendungsdienstprozesse, die auf dem Knoten ausgeführt werden. Standardwert ist 11000.
-MaxProcessPort -ma	Optional. Größte Portnummer für die Anwendungsdienstprozesse, die auf dem Knoten ausgeführt werden. Standardwert ist 11999.
-LogServiceDirectory -ld	Erforderlich. Freigegebener Verzeichnispfad, der vom Protokollmanager zum Speichern von Protokollereignisdateien verwendet wird. Stellen Sie sicher, dass -ld nicht übereinstimmt oder den angegebenen Wert für -sld enthält.
-SystemLogDirectory -sld	Optional. Verzeichnispfad zum Speichern von Systemprotokolldateien. Stellen Sie sicher, dass -ld nicht übereinstimmt oder den angegebenen Wert für -sld enthält. Standardwert ist <INFA_home>/logs.
-ServerPort -sv	Optional. Vom Dienstmanager verwendete TCP/IP-Portnummer. Der Dienstmanager verwaltet Befehle zum Herunterfahren aus PowerCenter-Komponenten auf diesem Port. Legen Sie diese Portnummer fest, wenn sich auf einem Computer mehrere Knoten befinden oder die Standardportnummer verwendet wird. Standardwert ist 8005.
-AdminconsoleShutdownPort -asp	Optional. Portnummer, die das Herunterfahren für Informatica Administrator steuert.

Option	Beschreibung
-BackupDirectory -bd	Optional. Verzeichnis zum Speichern der Repository-Backup-Dateien. Der Zugriff auf das Verzeichnis muss über den Knoten möglich sein.
-ErrorLogLevel -el	Optional. Schweregradstufe für Protokollereignisse im Domänenprotokoll. Standardwert ist „info“.
-ResourceFile -rf	Erforderlich. Datei, die eine Liste der verfügbaren Ressourcen für den Knoten enthält. Verwenden Sie die Datei „nodeoptions.xml“, die sich in folgendem Verzeichnis befindet: <INFA_HOME>\isp\bin.
-Tablespace -ts	Erforderlich für eine IBM DB2-Datenbank. Name des Tablespace, in dem sich die Datenbanktabellen für die Domänenkonfiguration befinden.
-SchemaName -sc	Optional. Name des Microsoft SQL Server-Schemas. Geben Sie einen Schemanamen ein, wenn Sie nicht das Standardschema verwenden.
-DatabaseTlsEnabled -dbtls	Optional. Gibt an, ob die Informatica-Domänenendatenbank mit TLS und SSL sicher ist. Setzen Sie diese Option für die sichere Datenbank auf True. Standardwert ist „False“. Wenn die Option „-dbtls“ ohne Wert angegeben wird, verwendet die Informatica-Domäne die sichere Kommunikation mit der Informatica-Domänenendatenbank.
-DatabaseTruststorePassword -dbtp	Optional. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.
-TrustedConnection -tc	Optional. Stellen Sie eine Verbindung zur Microsoft SQL Server-Datenbank über eine vertrauenswürdige Verbindung her. Die vertrauenswürdige Authentifizierung verwendet die Windows-Sicherheitsanmeldedaten des aktuellen Benutzers, um eine Verbindung zu Microsoft SQL Server herzustellen.
-DatabaseTruststoreLocation -dbtl	Pfad und Dateiname der Truststore-Datei für die sichere Domänenrepository-Datenbank. Erforderlich, wenn Sie eine sichere Domänenrepository-Datenbank für die Domäne konfigurieren.
* Hinweis: Wenn Sie derzeit Skripts ausführen, die diesen Befehl verwenden, um einen benutzerdefinierten Schlüsselspeicher für die SAML-Authentifizierung zu aktivieren, müssen Sie diese aktualisieren, um diese Option aufzunehmen.	

## VERWANDTE THEMEN:

- [“AddDomainNode” auf Seite 376](#)

# DefineWorkerNode

Definiert einen Arbeitsknoten auf dem aktuellen Computer. Infasetup erstellt die Datei „nodemeta.xml“, in der die Konfigurationsmetadaten für den Knoten gespeichert werden. Wenn Sie diesen Befehl auf einem vorhandenen Knoten ausführen, überschreibt er die Konfigurationsmetadaten des Knotens. Nachdem Sie den



Knoten definiert haben, führen Sie den Befehl `infacmd isp AddDomainNode` aus, um den Knoten zur Domäne hinzuzufügen.

Der Befehl „DefineWorkerNode“ verwendet die folgende Syntax:

```
DefineWorkerNode
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
<-NodeAddress|-na> node_host:port
[<-ServiceManagerPort|-sp> service_manager_port]
[<-EnableTLS|-tls> enable_tls]
[<-NodeKeystore|-nk> node_keystore_directory]
[<-NodeKeystorePass|-nkp> node_keystore_password]
[<-NodeTruststore|-nt> node_truststore_directory]
[<-NodeTruststorePass|-ntp> node_truststore_password]
[<-EnableKerberos|-krb> enable_kerberos]
[<-ServiceRealmName|-srn> realm_name_of_node_spn]
[<-UserRealmName|-urn> realm_name_of_user_spn]
[<-KeysDirectory|-kd> Infa_keys_directory_location]
[<-HttpsPort|-hs> admin_tool_https_port]
[<-NodeKeystoreFile|-kf> admin_tool_keystore_file_location]
[<-KeystorePass|-kp> admin_tool_keystore_password]
<-GatewayAddress|-dg> domain_gateway_host:port
[<-UserName|-un> user_name]
[<-SecurityDomain|-sdn> security_domain]
[<-Password|-pd> password]
[<-MinProcessPort|-mi> minimum_port]
[<-MaxProcessPort|-ma> maximum_port]
[<-ServerPort|-sv> server_shutdown_port]
[<-BackupDirectory|-bd> backup_directory]
[<-ErrorLogLevel|-el> FATAL_ERROR_WARNING_INFO_TRACE_DEBUG]
<-ResourceFile|-rf> resource_file
[<-SystemLogDirectory|-sld> system_log_directory]
[<-EnableSaml|-saml> enable_saml]
[<-SamlTrustStoreDir|-std> saml_truststore_directory]
[<-SamlTrustStorePassword|-stp> saml_truststore_password]
[<-SamlKeyStoreDir|-skd> saml_keystore_directory]
[<-SamlKeyStorePassword|-skp> saml_keystore_password]
```

In der folgenden Tabelle werden die Optionen und Argumente für „*infasetup* DefineWorkerNode“ beschrieben:

Option	Beschreibung
-DomainName -dn	Erforderlich. Name der Domäne, mit der der Arbeitsknoten verknüpft ist.
-NodeName -nn	Erforderlich. Name des Knotens. Knotennamen müssen zwischen 1 und 79 Zeichen umfassen und dürfen weder Leerzeichen noch die folgenden Zeichen enthalten: \ / * ? < > "
-NodeAddress -na	Erforderlich. Hostname und Portnummer für den Computer, auf dem der Knoten gehostet wird. Wählen Sie eine verfügbare Portnummer aus.
-ServiceManagerPort -sp	Optional. Portnummer, die vom Dienstmanager verwendet wird, um auf eingehende Verbindungsanfragen zu reagieren.

Option	Beschreibung
-EnableTLS -tls	<p>Optional. Konfiguriert die sichere Kommunikation für die Dienste in der Informatica-Domäne.</p> <p>Wenn Sie die standardmäßigen, von Informatica bereitgestellten SSL-Zertifikate verwenden, müssen Sie die Schlüsselspeicher- und Truststore-Optionen nicht angeben. Wenn Sie das SSL-Zertifikat nicht verwenden, müssen Sie die Keystore- und Truststore-Optionen angeben. Gültige Werte sind „True“ oder „False“. Standardwert ist „False“. Wenn Sie die Option -tls ohne Wert angeben, verwendet die Informatica-Domäne die sichere Kommunikation zwischen Diensten.</p> <p>Zum Aktivieren der sicheren Kommunikation für die verbundenen Dienste oder Webanwendungen, z. B. das Administrator Tool, das Analyst Tool oder den Webdienst-Hub, konfigurieren Sie die sichere Kommunikation separat innerhalb der Anwendungen.</p>
-NodeKeystore -nk	<p>Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Verzeichnis, das die Schlüsselspeicherdateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS-Dateien (Java Keystore) vorliegen. Das Verzeichnis muss Schlüsselspeicherdateien in den Formaten PEM und JKS enthalten.</p> <p>Die Schlüsselspeicherdateien müssen infa_keystore.jks und infa_keystore.pem lauten. Wenn die Schlüsselspeicherdatei, die Sie von der Zertifizierungsstelle erhalten, einen anderen Namen hat, müssen Sie sie in infa_keystore.jks und infa_keystore.pem umbenennen.</p> <p>Sie müssen für alle Knoten in der Domäne dieselben Schlüsselspeicherzertifikate verwenden.</p>
-NodeKeystorePass -nkp	<p>Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die Schlüsselspeicherdatei infa_keystore.jks.</p>
-NodeTruststore -nt	<p>Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Verzeichnis, das die Truststore-Dateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS-Dateien (Java Keystore) vorliegen. Das Verzeichnis muss Truststore-Dateien in den Formaten PEM und JKS enthalten.</p> <p>Die Truststore-Dateien müssen die Namen infa_truststore.jks und infa_truststore.pem aufweisen. Wenn die Truststore-Datei, die Sie von der Zertifizierungsstelle erhalten haben, einen anderen Namen aufweist, müssen Sie sie in infa_truststore.jks und infa_truststore.pem umbenennen.</p>
-NodeTruststorePass -ntp	<p>Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die Datei infa_truststore.jks.</p>
-CipherWhiteList -cwl	<p>Optional. Eine kommagetrennte Liste mit JSSE-Chiffre-Suites, die zur Gültigkeitsliste hinzugefügt werden sollen.</p> <p><b>Hinweis:</b> Die Liste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.</p>
-CipherBlackList -cbl	<p>Optional. Eine kommagetrennte Liste mit JSSE-Chiffre-Suites, die aus der Gültigkeitsliste entfernt werden sollen.</p> <p><b>Hinweis:</b> Die Gültigkeitsliste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.</p>
-CipherWhiteListFile -cwlf	<p>Optional. Absoluter Dateiname der Klartextdatei, die eine kommagetrennte Liste mit Chiffre-Suites enthält, die der Gültigkeitsliste hinzugefügt werden sollen.</p> <p><b>Hinweis:</b> Die Liste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.</p>

Option	Beschreibung
-CipherBlackListFile -cblf	Optional. Absoluter Dateiname der Klartextdatei, die eine kommagetrennte Liste mit Chiffre-Suites enthält, die aus der Gültigkeitsliste entfernt werden sollen. <b>Hinweis:</b> Die Gültigkeitsliste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-EnableKerberos -krb	Optional. Konfiguriert die Informatica-Domäne zur Verwendung der Kerberos-Authentifizierung. Gültige Werte sind „True“ oder „False“. Bei True verwendet die Domäne die Kerberos-Authentifizierung, dann können Sie den Authentifizierungsmodus später nicht ändern. Nachdem Sie die Kerberos-Authentifizierung aktiviert haben, können Sie sie nicht deaktivieren. Standardwert ist „False“. Wenn Sie die Option -krb ohne einen Wert angeben, verwendet die Informatica-Domäne die Kerberos-Authentifizierung.
-ServiceRealmName -srn	Optional. Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung. Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie die Namen aller Kerberos-Bereiche, die von der Domäne zum Authentifizieren von Benutzern verwendet werden, getrennt durch Kommas ein. Beispiel: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Geben Sie beispielsweise folgenden Wert an, um alle Bereiche einzuschließen, die den Namen EAST.COMPANY.COM enthalten: *EAST.COMPANY.COM
-UserRealmName -urn	Optional. Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung. Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie die Namen aller Kerberos-Bereiche, die von der Domäne zum Authentifizieren von Benutzern verwendet werden, getrennt durch Kommas ein. Beispiel: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Geben Sie beispielsweise folgenden Wert an, um alle Bereiche einzuschließen, die den Namen EAST.COMPANY.COM enthalten: *EAST.COMPANY.COM
-KeysDirectory -kd	Optional. Verzeichnis, in dem alle Schlüsseltabellendateien und der Verschlüsselungsschlüssel für die Informatica-Domäne gespeichert werden. Standardwert ist <Informatica-Installationsverzeichnis>/isp/config/keys.
-HttpsPort -hs	Optional. Portnummer, die vom Knoten für die Kommunikation zwischen dem Administrator Tool und dem Dienstmanager verwendet wird. Geben Sie diese Portnummer an, wenn Sie HTTPS für einen Knoten konfigurieren möchten. Zum Deaktivieren von HTTPS-Unterstützung für einen Knoten setzen Sie diese Portnummer auf Null.
-NodeKeystoreFile -kf	Optional. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die bei Verwendung des SSL-Protokolls erforderlich sind
-KeystorePass -kp	Optional. Ein Klartext-Passwort für die Schlüsselspeicherdatei. Sie können ein Passwort mit der Option -kp oder der Umgebungsvariable INFA_PASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -kp festgelegte Passwort Vorrang.

Option	Beschreibung
-GatewayAddress -dg	Erforderlich. Name und Portnummer des Gateway-Hostcomputers.
-UserName -un	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-SecurityDomain -sdn	<p>Name der Sicherheitsdomäne, die Sie erstellen möchten und zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Sie können einen Wert für -sdn angeben oder den Standardwert basierend auf dem Authentifizierungsmodus verwenden:</p> <ul style="list-style-type: none"> <li>- Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Standardwert ist „Nativ“. Zum Arbeiten mit der LDAP-Authentifizierung müssen Sie den Wert für -sdn angeben.</li> <li>- Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Standardwert ist „Native“ für native Authentifizierung. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</li> </ul>
-Password -pd	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-MinProcessPort -mi	Optional. Kleinste Portnummer für die Anwendungsdienstprozesse, die auf dem Knoten ausgeführt werden. Standardwert ist 11000.
-MaxProcessPort -ma	Optional. Größte Portnummer für die Anwendungsdienstprozesse, die auf dem Knoten ausgeführt werden. Standardwert ist 11999.
-ServerPort -sv	Optional. Vom Dienstmanager verwendete TCP/IP-Portnummer. Der Dienstmanager verwaltet Befehle zum Herunterfahren aus PowerCenter-Komponenten auf diesem Port. Legen Sie diese Portnummer fest, wenn sich auf einem Computer mehrere Knoten befinden oder die Standardportnummer verwendet wird. Standardwert ist 8005.
-BackupDirectory -bd	Optional. Verzeichnis zum Speichern der Repository-Backup-Dateien. Der Zugriff auf das Verzeichnis muss über den Knoten möglich sein.

Option	Beschreibung
-ErrorLogLevel -el	Optional. Schweregradstufe für Protokollereignisse im Domänenprotokoll. Eine der folgenden Optionen: <ul style="list-style-type: none"> <li>- fatal</li> <li>- error</li> <li>- warning</li> <li>- info</li> <li>- trace</li> <li>- debug</li> </ul> Standardwert ist „info“.
-ResourceFile -rf	Erforderlich. Datei, die eine Liste der verfügbaren Ressourcen für den Knoten enthält. Verwenden Sie die Datei „nodeoptions.xml“, die sich in folgendem Verzeichnis befindet: <INFA_HOME>\isp\bin.
-SystemLogDirectory -sld	Optional. Verzeichnispfad zum Speichern von Systemprotokolldateien. Standardwert ist <INFA_home>/logs.
-EnableSaml -saml	Optional. Aktiviert oder deaktiviert die SAML-Authentifizierung in der Informatica-Domäne. Legen Sie diesen Wert auf „true“ fest, um die SAML-Authentifizierung in der Informatica-Domäne zu aktivieren. Der Standardwert ist „false“.
-SamlTrustStoreDir -std	Optional. Das Verzeichnis mit der benutzerdefinierten Truststore-Datei, die für die Verwendung der SAML-Authentifizierung auf dem Gateway-Knoten erforderlich ist. Geben Sie nur das Verzeichnis an, nicht den vollständigen Pfad zur Datei. Der Informatica-Standard-Truststore wird verwendet, wenn kein Truststore angegeben ist.
-SamlTrustStorePassword -stp	Erforderlich, wenn Sie einen benutzerdefinierten Truststore für die SAML-Authentifizierung verwenden. Das Passwort für den benutzerdefinierten Truststore.
-SamlKeyStoreDir -skd	Optional. Das Verzeichnis mit der benutzerdefinierten Truststore-Datei, die für die Verwendung der SAML-Authentifizierung auf dem Gateway-Knoten erforderlich ist. Geben Sie nur das Verzeichnis an, nicht den vollständigen Pfad zur Datei.
-SamlKeyStorePassword -skp	Erforderlich, wenn Sie einen benutzerdefinierten Schlüsselspeicher für die SAML-Authentifizierung verwenden. Passwort für den SAML-Schlüsselspeicher. *
* Hinweis: Wenn Sie derzeit Skripts ausführen, die diesen Befehl verwenden, um einen benutzerdefinierten Schlüsselspeicher für die SAML-Authentifizierung zu aktivieren, müssen Sie diese aktualisieren, um diese Option aufzunehmen.	

## DeleteDomain

Löscht Metadatentabellen der Domäne. Vor dem Ausführen dieses Befehls müssen Sie die Informatica-Dienste auf dem Computer beenden. Zum Löschen einer Domäne auf einem Windows-Computer müssen Sie ebenfalls den Hostport öffnen oder die Firewall deaktivieren.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, stellen Sie für „infasetup“ mehr Systemspeicher zur Verfügung. Um mehr Systemspeicher zur Verfügung zu stellen, geben Sie den -Xmx-Wert in der Umgebungsvariable INFA\_JAVA\_CMD\_OPTS an.

Der Befehl „DeleteDomain“ verwendet die folgende Syntax:

```

DeleteDomain

<<-DatabaseAddress|-da> database_hostname:database_port|

<-DatabaseConnectionString|-cs> database_connection_string>

[<-DatabaseUserName|-du> database_user_name]

[<-DatabasePassword|-dp> database_password]

<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE|POSTGRESQL

[<-DatabaseServiceName|-ds> database_service_name]

[<-Tablespace|-ts> tablespace_name]

[<-SchemaName|-sc> schema_name (used for Microsoft SQL Server and PostgreSQL only)]

[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]

[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]

[<-TrustedConnection|-tc> trusted_connection (used for Microsoft SQL Server only)]

[<-EncryptionKeyLocation|-kl> encryption_key_location]

[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]

```

In der folgenden Tabelle werden die Optionen und Argumente für „infasetup DeleteDomain“ beschrieben:

Option	Argument	Beschreibung
-DatabaseAddress -da	database_hostname:database_port	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Name und Portnummer des Computers, auf dem die Konfigurationsdatenbank der Domäne gehostet wird.
-DatabaseConnectionString -cs	database_connection_string	Erforderlich, wenn Sie die Optionen -DatabaseAddress (-da) und -DatabaseServiceName (-ds) nicht verwenden. Verbindungszeichenfolge, die zum Herstellen einer Verbindung zur Konfigurationsdatenbank der Domäne verwendet wird. Geben Sie den Namen des Datenbankhosts, -ports und -diensts als Teil der Verbindungszeichenfolge ein. Setzen Sie die Verbindungszeichenfolge in Anführungszeichen.
-DatabaseUserName -du	database_user_name	Erforderlich, wenn Sie die Option -TrustedConnection (-tc) nicht verwenden. Konto für die Datenbank, die die Domänenkonfigurationsinformationen enthält.

Option	Argument	Beschreibung
-DatabasePassword -dp	database_password	Passwort aus der Datenbank für die Domänenkonfiguration des Datenbankbenutzers. Wenn Sie diese Option weglassen, verwendet <i>infasetup</i> das in der Umgebungsvariable <code>INFA_DEFAULT_DATABASE_PASSWORD</code> angegebene Passwort. Wird in der Umgebungsvariable kein Wert angegeben, müssen Sie ein Passwort unter Verwendung dieser Option eingeben.
-DatabaseType -dt	database_type	Erforderlich. Typ der Datenbank, in der die Domänenkonfigurationsmetadaten gespeichert werden. Zu den Datenbanktypen gehören: <ul style="list-style-type: none"> <li>- db2</li> <li>- oracle</li> <li>- mssqlserver</li> <li>- sybase</li> <li>- postgresql</li> </ul>
-DatabaseServiceName -ds	database_service_name	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Der Name des Datenbankdiensts. Erforderlich für Oracle-, IBM DB2- und Microsoft SQL Server-Datenbanken. Geben Sie die SID für Oracle, den Dienstnamen für IBM DB2 oder den Datenbanknamen für Microsoft SQL Server ein.
-Tablespace -ts	tablespace_name	Erforderlich für eine IBM DB2-Datenbank. Name des Tablespace, in dem sich die Datenbanktabellen für die Domänenkonfiguration befinden.
SchemaName -sc	schema_name	Optional. Name des Microsoft SQL Server- oder des PostgreSQL-Schemas. Geben Sie einen Schemanamen ein, wenn Sie nicht das Standardschema verwenden.
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Optional. Gibt an, ob die Informatica-Domänendatenbank mit TLS und SSL sicher ist. Setzen Sie diese Option für die sichere Datenbank auf True. Standardwert ist „False“. Wenn die Option -dbtls ohne Wert angegeben wird, verwendet die Informatica-Domäne die sichere Kommunikation mit der Informatica-Domänendatenbank.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Optional. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.
-TrustedConnection -tc	-	Optional. Stellen Sie eine Verbindung zur Microsoft SQL Server-Datenbank über eine vertrauenswürdige Verbindung her. Die vertrauenswürdige Authentifizierung verwendet die Windows-Sicherheitsanmeldedaten des aktuellen Benutzers, um eine Verbindung zu Microsoft SQL Server herzustellen.

Option	Argument	Beschreibung
-EncryptionKeyLocation -kl	encryption_key_location	Verzeichnis, das den aktuellen Verschlüsselungsschlüssel enthält. Der Name der Verschlüsselungsdatei lautet „sitekey“. Informatica benennt die aktuelle sitekey-Datei in sitekey_old um und generiert einen Verschlüsselungsschlüssel in einer neuen Datei mit dem Namen sitekey in demselben Verzeichnis.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Pfad und Dateiname der Truststore-Datei für die sichere Domänenrepository-Datenbank. Erforderlich, wenn Sie eine sichere Domänenrepository-Datenbank für die Domäne konfigurieren.

## GenerateEncryptionKey

Generieren Sie einen Verschlüsselungsschlüssel, um vertrauliche Daten wie Passwörter in der Informatica-Domäne zu sichern.

Der Befehl `GenerateEncryptionKey` verwendet die folgende Syntax:

```
GenerateEncryptionKey [<-EncryptionKeyLocation|-kl> encryption_key_location]
```

**-EncryptionKeyLocation.** Verzeichnis, das den aktuellen Verschlüsselungsschlüssel enthält. Der Name der Verschlüsselungsdatei lautet *sitekey*. Informatica benennt die aktuelle *sitekey*-Datei in *sitekey\_old* um und generiert einen Verschlüsselungsschlüssel in einer neuen Datei mit dem Namen *sitekey* im selben Verzeichnis.

Um den Befehl erneut auszuführen, wenn mindestens zwei *sitekey*-Dateien im Verzeichnis vorhanden sind, stellen Sie sicher, dass Sie die *sitekey*-Dateien sichern. Sie können anschließend den Befehl zum Erstellen der *sitekey*-Datei ausführen, bevor Sie die *sitekey*-Dateien aus der Sicherung wiederherstellen.

Der *sitekey* ist eindeutig. Stellen Sie sicher, dass Sie eine Kopie dieses eindeutigen Sitekeys speichern. Wenn Sie den Sitekey verlieren, können Sie ihn nicht erneut generieren. Teilen Sie den eindeutigen Sitekey nicht mit anderen.

## Hilfe

Der Befehl `Help` zeigt die Optionen und Argumente für einen Befehl an. Wenn Sie den Befehlsnamen weglassen, listet *infasetup* alle Befehle auf.

Der Befehl `Help` verwendet die folgende Syntax:

```
Help [command]
```



Wenn Sie beispielsweise `infasetup Help UpdateWorkerNode` eingeben, gibt *infasetup* die folgenden Optionen und Argumente für den Befehl `UpdateWorkerNode` zurück:

```
UpdateWorkerNode [<-DomainName|-dn> domain_name] [<-NodeName|-nn> node_name] [<-
NodeAddress|-na> node_host:port]
[<-GatewayAddress|-dg> domain_gateway_host:port] [<-UserName|-un> user_name] [<-Password|-
pd> password] [<-ServerPort|-sv> server_admin_port_number]
```

In der folgenden Tabelle werden die *infasetup* Help-Option und das -Argument beschrieben:

Option	Argument	Beschreibung
-	Befehl	Optional. Name des Befehls. Wenn Sie den Befehlsnamen weglassen, listet <i>infasetup</i> alle Befehle auf.

## ListDomainCiphers

Display one or more of the following cipher suite lists: blacklist, default list, effective list, or whitelist.

### Blacklist

Liste mit Chiffre-Suites, die von der Informatica-Domäne blockiert werden sollen. Wenn Sie der Blacklist eine Chiffre-Suite hinzufügen, entfernt die Informatica-Domäne diese Chiffre-Suite aus der Gültigkeitsliste. Sie können Chiffre-Suites, die sich in der Standardliste befinden, zur Blacklist hinzufügen.

### Standardliste

Liste mit Chiffre-Suites, die von der Informatica-Domäne standardmäßig unterstützt werden.

### Whitelist

Liste mit Chiffre-Suites, die von der Informatica-Domäne zusätzlich zu denen in der Standardliste unterstützt werden sollen. Wenn Sie der Whitelist eine Chiffre-Suite hinzufügen, fügt die Informatica-Domäne die Chiffre-Suite zur Gültigkeitsliste hinzu. Chiffre-Suites, die sich in der Standardliste befinden, müssen nicht zur Whitelist hinzugefügt werden.

The `ListDomainCiphers` command uses the following syntax:

```
[<-list|-l>] ALL|BLACK|DEFAULT|EFFECTIVE|WHITE
[<-domainConfig|-dc> true|false]
```

**Hinweis:** You cannot run this command on a worker node.

The following table describes infasetup listDomainCiphers options and arguments:

Option	Argument	Description
-list -l	ALL BLACK DEFAULT EFFECTIVE WHITE	Optional. The cipher suite configuration list to display. The argument ALL displays the blacklist, default list, effective list, and whitelist. The argument BLACK displays the blacklist. The argument DEFAULT displays the default list. The argument EFFECTIVE displays the effective list. The argument WHITE displays the whitelist. <b>Hinweis:</b> The arguments are case-sensitive. When you run the command on a gateway node and omit this option, the command displays all cipher suite configuration lists.
-domainConfig -dc	true false	Optional. Display the cipher suite lists for the Informatica domain or for the gateway node where you run the command. By default, the command displays cipher suite lists for the domain. Set this option to true to display the cipher suite lists for the domain. Set this option to false to display the cipher suite list for the gateway node where you run the command. <b>Hinweis:</b> You cannot view whitelists or blacklists on gateway nodes.

## MigrateEncryptionKey

Ändern Sie den Verschlüsselungsschlüssel, um vertrauliche Daten wie Passwörter in der Informatica-Domäne zu sichern.

```
MigrateEncryptionKey  
  
<-LocationOfEncryptionKeys|-loc> location_of_encryption_keys  
  
[<-IsDomainMigrated|-mig> is_domain_migrated]
```

In der folgenden Tabelle werden *infasetup MigrateEncryptionKey* beschrieben:

Option	Argument	Beschreibung
-LocationOfEncryptionKeys -loc	location_of_encryption_keys	<p>Erforderlich. Verzeichnis, in dem die alte Verschlüsselungsschlüsseldatei mit der Bezeichnung „siteKey_old“ und die neue Verschlüsselungsschlüsseldatei mit der Bezeichnung „siteKey“ gespeichert sind.</p> <p>Das Verzeichnis muss die alten und neuen Verschlüsselungsschlüsseldateien enthalten. Wenn die alten und neuen Verschlüsselungsschlüsseldateien in verschiedenen Verzeichnissen gespeichert werden, kopieren Sie die Verschlüsselungsschlüsseldateien in dasselbe Verzeichnis.</p> <p>Wenn die Domäne mehrere Knoten enthält, muss dieses Verzeichnis allen Knoten in der Domäne zugänglich sein, in der Sie den Befehl „migrateEncryptionKey“ ausführen.</p>
-IsDomainMigrated -mig	is_domain_migrated	<p>Optional. Gibt an, ob die Domäne für die Verwendung des neuesten Verschlüsselungsschlüssels aktualisiert wurde.</p> <p>Beim erstmaligen Ausführen des Befehls „migrateEncryptionKey“ legen Sie diese Option auf FALSE fest, um anzugeben, dass die Domäne den alten Verschlüsselungsschlüssel verwendet.</p> <p>Nach dem erstmaligen Ausführen des Befehls „migrateEncryptionKey“ zum Aktualisieren anderer Knoten in der Domäne setzen Sie diese Option auf TRUE fest, um anzugeben, dass die Domäne für die Verwendung des neuesten Verschlüsselungsschlüssels aktualisiert wurde. Sie können den Befehl „migrateEncryptionKey“ auch ohne diese Option ausführen.</p> <p>Standardwert ist „True“.</p>

## RestoreDomain

Stelle die Konfigurationsmetadaten für die Domäne aus einer .mrep-Backup-Datei wieder her. Wenn Sie über eine Backup-Datei aus einer früheren Informatica-Version verfügen, müssen Sie die frühere Version zum Wiederherstellen der Domäne verwenden.

Sie müssen die Domäne vor dem Ausführen dieses Befehls herunterfahren.

Wenn Sie die Domäne in einer anderen als der ursprünglichen Backup-Datenbank wiederherstellen, müssen Sie die Inhalte der Tabelle ISP\_RUN\_LOG wiederherstellen, um die früheren Arbeitsablaufs- und Sitzungsprotokolle zu erhalten.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, stellen Sie für „infasetup“ mehr Systemspeicher zur Verfügung. Um mehr Systemspeicher zur Verfügung zu stellen, geben Sie den -Xmx-Wert in der Umgebungsvariable INFA\_JAVA\_CMD\_OPTS an.

Der Befehl „RestoreDomain“ verwendet die folgende Syntax:

```
RestoreDomain

<<-DatabaseAddress|-da> database_hostname:database_port|

<-DatabaseConnectionString|-cs> database_connection_string>

[<-DatabaseUserName|-du> database_user_name]

[<-DatabasePassword|-dp> database_password]

<-DatabaseType|-dt> database_type

[<-DatabaseServiceName|-ds> database_service_name]

<-BackupFile|-bf> backup_file_name

[<-Force|-f>]

[<-ClearNodeAssociation|-ca>]

[<-Tablespace|-ts> tablespace_name]

[<-SchemaName|-sc> schema_name (used for MSSQLServer and PostgreSQL only)]

[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]

[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]

[<-TrustedConnection|-tc> trusted_connection (used for MSSQLServer only)]

[<-EncryptionKeyLocation|-kl> encryption_key_location]

[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
```

In der folgenden Tabelle werden *infasetup* RestoreDomain“ beschrieben:

Option	Argument	Beschreibung
-DatabaseAddress -da	database_hostname:database_port	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Name und Portnummer des Computers, auf dem die Konfigurationsdatenbank der Domäne gehostet wird.
-DatabaseConnectionString -cs	database_connection_string	Erforderlich, wenn Sie die Optionen -DatabaseAddress (-da) und -DatabaseServiceName (-ds) nicht verwenden. Verbindungszeichenfolge, die zum Herstellen einer Verbindung zur Konfigurationsdatenbank der Domäne verwendet wird. Geben Sie den Namen des Datenbankhosts, -ports und -diensts als Teil der Verbindungszeichenfolge ein. Setzen Sie die Verbindungszeichenfolge in Anführungszeichen.
-DatabaseUserName -du	database_user_name	Erforderlich, wenn Sie die Option -TrustedConnection (-tc) nicht verwenden. Konto für die Datenbank, die die Domänenkonfigurationsinformationen enthält.

Option	Argument	Beschreibung
-DatabasePassword -dp	database_password	Passwort aus der Datenbank für die Domänenkonfiguration des Datenbankbenutzers. Wenn Sie diese Option weglassen, verwendet <i>infasetup</i> das in der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD angegebene Passwort. Wird in der Umgebungsvariable kein Wert angegeben, müssen Sie ein Passwort unter Verwendung dieser Option eingeben.
-DatabaseType -dt	database_type	Erforderlich. Typ der Datenbank, in der die Domänenkonfigurationsmetadaten gespeichert werden. Zu den Datenbanktypen gehören: <ul style="list-style-type: none"> <li>- db2</li> <li>- oracle</li> <li>- mssqlserver</li> <li>- sybase</li> <li>- postgresql</li> </ul>
-DatabaseServiceName -ds	database_service_name	Erforderlich, wenn Sie die Option - DatabaseConnectionString (-cs) nicht verwenden. Der Name des Datenbankdiensts. Erforderlich für Oracle-, IBM DB2- und Microsoft SQL Server-Datenbanken. Geben Sie die SID für Oracle, den Dienstnamen für IBM DB2 oder den Datenbanknamen für Microsoft SQL Server ein.
-BackupFile -bf	backup_file_name	Erforderlich. Name und Pfad der Backup-Datei. Wenn Sie keinen Dateipfad angeben, erstellt <i>infasetup</i> die Backup-Datei im aktuellen Verzeichnis.
-Force -f	-	Optional. Überschreibt die Datenbank, wenn eine Datenbank mit demselben Namen bereits vorhanden ist. Geben Sie im Anschluss an diese Option keine weiteren Zeichen ein.
-ClearNodeAssociation -ca	-	Optional. Löscht Knotenzuordnungen beim Wiederherstellen der Domäne. Eine gesicherte Domäne enthält beispielsweise den Knoten „Node1“ auf dem Computer „MyHost:9090“. Wenn Sie diese Option auswählen, wird die Verbindung zwischen dem Knotennamen „Node1“ und der Adresse „MyHost:9090“ beim Wiederherstellen der Domäne unterbrochen. Sie können dann „MyHost:9090“ einen anderen Knoten zuordnen.  Wenn Sie diese Option nicht angeben, behält „Node1“ die Verbindung zu „MyHost:9090“ bei. Wenn Sie die Domäne wiederherstellen und „MyHost:9090“ einen anderen Knoten zuordnen, wird der Knoten nicht gestartet.
-Tablespace -ts	tablespace_name	Erforderlich für eine IBM DB2-Datenbank. Name des Tablespace, in dem sich die Datenbanktabellen für die Domänenkonfiguration befinden.
-SchemaName -sc	schema_name	Optional. Name des Microsoft SQL Server- oder des PostgreSQL-Schemas. Geben Sie einen Schemanamen ein, wenn Sie nicht das Standardschema verwenden.

Option	Argument	Beschreibung
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Optional. Gibt an, ob die Informatica-Domänendatenbank mit TLS und SSL sicher ist. Setzen Sie diese Option für die sichere Datenbank auf True. Standardwert ist „False“. Wenn die Option -dbtls ohne Wert angegeben wird, verwendet die Informatica-Domäne die sichere Kommunikation mit der Informatica-Domänendatenbank.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Optional. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.
-TrustedConnection -tc	-	Optional. Stellen Sie eine Verbindung zur Microsoft SQL Server-Datenbank über eine vertrauenswürdige Verbindung her. Die vertrauenswürdige Authentifizierung verwendet die Windows-Sicherheitsanmeldedaten des aktuellen Benutzers, um eine Verbindung zu Microsoft SQL Server herzustellen.
-EncryptionKeyLocation -kl	encryption_key_location	Optional. Verzeichnis, das den aktuellen Verschlüsselungsschlüssel enthält. Sie müssen den Schlüsselspeicherort angeben, wenn der Verschlüsselungsschlüssel nicht in der Datei „isp/config/keys/sitekey“ vorhanden ist. Der Name der Verschlüsselungsdatei lautet „sitekey“.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Optional. Pfad und Dateiname der Truststore-Datei für die sichere Datenbank. Erforderlich, wenn Sie eine sichere Domänenrepository-Datenbank für die Domäne konfigurieren.

## restoreMitKerberosLinkage

Stellt die Verknüpfungen zu den Kerberos-Standardbibliotheken wieder her, die in der Informatica-Domäne für Kerberos-Authentifizierung verwendet werden. Der Befehl entfernt auch Verknüpfungen zu allen benutzerdefinierten Kerberos-Bibliotheken, die innerhalb der Informatica-Domäne vorhanden sind.

Gehen Sie zum Verwenden der Kerberos-Standardbibliotheken in einer Informatica-Domäne folgendermaßen vor:

1. Fahren Sie die Domäne herunter.
2. Führen Sie den Befehl „infasetup restoreMitKerberosLinkage“ auf jedem Knoten in der Domäne aus.
3. Starten Sie die Domäne, nachdem der Befehl auf allen Knoten in der Domäne ausgeführt wurde.

Der Befehl verwendet keine Optionen oder Argumente. Sie müssen über Lese- und Schreibberechtigungen auf allen Knoten in der Informatica-Domäne verfügen, um den Befehl auszuführen.

# SwitchToKerberosMode

Konfigurieren Sie die Informatica-Domäne zur Verwendung der Kerberos-Authentifizierung.

Der Befehl SwitchToKerberosMode verwendet die folgende Syntax:

```
SwitchToKerberosMode  
  
<-administratorName|-ad> administrator_name  
  
<-ServiceRealmName|-srn> realm_name_of_node_spn  
  
<-UserRealmName|-urn> realm_name_of_user_spn  
  
[<-SPNShareLevel|-spnSL> SPNShareLevel PROCESS|NODE]
```

In der folgenden Tabelle werden *infasetup* SwitchToKerberosMode-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-administratorName -ad	administrator_name	<p>Erforderlich. Benutzername für das Domänenadministrator-Konto, das beim Konfigurieren der Kerberos-Authentifizierung erstellt wird. Geben Sie den Namen eines Kontos an, das in Active Directory vorhanden ist.</p> <p>Nachdem Sie die Kerberos-Authentifizierung konfiguriert haben, wird dieser Benutzer in die Sicherheitsdomäne <i>_infalInternalNamespace</i> aufgenommen, die vom Befehl erstellt wird.</p> <p>Wenn die Domäne einen einzelnen Kerberos-Bereich zum Authentifizieren von Benutzern verwendet, geben Sie den SAM-Kontonamen an.</p> <p>Wenn die Domäne die bereichsübergreifende Kerberos-Authentifizierung verwendet, geben Sie den vollqualifizierten Benutzerprinzipalnamen, einschließlich des Bereichsnamens, an. Beispiel: <code>sysadmin@COMPANY.COM</code></p>
-ServiceRealmName -srn	realm_name_of_node_spn n	<p>Erforderlich. Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung.</p> <p>Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie die Namen aller Kerberos-Bereiche, die von der Domäne zum Authentifizieren von Benutzern verwendet werden, getrennt durch Kommas ein. Beispiel: <code>COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</code></p> <p>Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Geben Sie beispielsweise folgenden Wert an, um alle Bereiche einzuschließen, die den Namen <code>EAST.COMPANY.COM</code> enthalten: <code>*EAST.COMPANY.COM</code></p>

Option	Argument	Beschreibung
-UserRealmName -urn	realm_name_of_user_sp n	<p>Erforderlich. Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/ Kleinschreibung.</p> <p>Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie die Namen aller Kerberos-Bereiche, die von der Domäne zum Authentifizieren von Benutzern verwendet werden, getrennt durch Kommas ein. Beispiel:</p> <p>COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Geben Sie beispielsweise folgenden Wert an, um alle Bereiche einzuschließen, die den Namen EAST.COMPANY.COM enthalten:</p> <p>*EAST.COMPANY.COM</p>
SPNShareLevel -spnSL	SPNShareLevel PROCESS [NODE]	<p>Optional. Gibt die Dienst-Prinzipalebene für die Domäne an. Legen Sie eine der folgenden Ebenen für die Eigenschaft fest:</p> <ul style="list-style-type: none"> <li>- Prozess Die Domäne erfordert einen eindeutigen Dienst-Prinzipalnamen (SPN) und eine Keytab-Datei für jeden Knoten und für jeden Dienst auf einem Knoten. Die Anzahl der pro Knoten erforderlichen SPNs und Keytab-Dateien hängt von der Anzahl der Dienstprozesse ab, die auf dem Knoten ausgeführt werden. Empfohlen für Produktionsdomänen.</li> <li>- Knoten. Die Domäne verwendet einen SPN und eine Keytab-Datei für den Knoten und für alle Dienste, die auf dem Knoten ausgeführt werden. Sie erfordert außerdem einen separaten SPN und eine separate Keytab-Datei für alle HTTP-Prozesse auf dem Knoten. Empfohlen für Test- und Entwicklungsdomänen. Empfohlen für Test- und Entwicklungsdomänen.</li> </ul> <p>Standardwert ist „Prozess“.</p>

## UpdateDomainCiphers

Dient zur Aktualisierung der Informatica-Domäne für die Verwendung einer neuen Gültigkeitsliste. Ändert die Whitelist, um Chiffre-Suites in die Gültigkeitsliste aufzunehmen. Ändert die Blacklist, um Chiffre-Suites aus der Gültigkeitsliste zu entfernen.

Überprüfen Sie vor der Ausführung dieses Befehls, ob die folgenden Voraussetzungen erfüllt werden:

- Für die Domäne werden intern sichere Kommunikation bzw. extern sichere Verbindungen mit Webclients verwendet.
- Die Domäne wurde heruntergefahren.
- Sie können den Befehl auf einem Gateway-Knoten in der Domäne ausführen.



Die Gültigkeitsliste mit Chiffre-Suites enthält die von der Informatica-Domäne unterstützten Chiffre-Suites. Beim Ausführen des Befehls „UpdateDomainCiphers“ erstellt die Informatica-Domäne die Gültigkeitsliste mit Chiffre-Suites auf Grundlage der folgenden Listen:

#### **Blacklist**

Liste mit Chiffre-Suites, die von der Informatica-Domäne blockiert werden sollen. Wenn Sie der Blacklist eine Chiffre-Suite hinzufügen, entfernt die Informatica-Domäne diese Chiffre-Suite aus der Gültigkeitsliste. Sie können Chiffre-Suites, die sich in der Standardliste befinden, zur Blacklist hinzufügen.

#### **Standardliste**

Liste mit Chiffre-Suites, die von der Informatica-Domäne standardmäßig unterstützt werden.

#### **Whitelist**

Liste mit Chiffre-Suites, die von der Informatica-Domäne zusätzlich zu denen in der Standardliste unterstützt werden sollen. Wenn Sie der Whitelist eine Chiffre-Suite hinzufügen, fügt die Informatica-Domäne die Chiffre-Suite zur Gültigkeitsliste hinzu. Chiffre-Suites, die sich in der Standardliste befinden, müssen nicht zur Whitelist hinzugefügt werden.

Beachten Sie die folgenden Richtlinien für die Ausführung des Befehls „UpdateDomainCiphers“:

- Beim Ausführen des Befehls erstellen Sie eine neue Gültigkeitsliste, die die bisherige überschreibt.
- Wenn Sie den Befehl ausführen und eine Whitelist oder Blacklist festlegen, überschreibt diese neue Liste die bisherige.
- Die Gültigkeitsliste umfasst die Chiffre-Suites, die sich in der Standardliste und Whitelist befinden, und schließt die Chiffre-Suites in der Blacklist aus.
- Wenn Sie den Befehl ausführen, ohne eine Whitelist oder Blacklist festzulegen, wird mit dem Befehl eine Gültigkeitsliste erstellt, die die Chiffre-Suites aus der Standardliste verwendet.
- Die Gültigkeitsliste muss mindestens eine Chiffre-Suite enthalten, die von TLS v1.1 oder 1.2 unterstützt wird.
- Bei der Gültigkeitsliste muss es sich um eine gültige Chiffre-Suite für Windows, die Java-Laufzeitumgebung und OpenSSL handeln.

Weitere Informationen zum Erstellen von Whitelists und Blacklists für die Aktualisierung der von der Informatica-Domäne verwendeten Gültigkeitsliste finden Sie im *Informatica-Sicherheitshandbuch*.

Für den Befehl „UpdateDomainCiphers“ wird die folgende Syntax verwendet:

```
[<-preview|-p> true|false]
[<-cipherWhiteList|-cwl> ciphersuite1,ciphersuite2,...]
[<-cipherWhiteListFile|-cwlf> whitelist_file_name]
[<-cipherBlackList|-cbl> ciphersuite1,ciphersuite2,...]
[<-cipherBlackListFile|-cblf> blacklist_file_name]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infasetup UpdateDomainCiphers“ beschrieben:

Option	Argument	Beschreibung
-preview -p	True Falsch	Optional. Bei „true“ wird mit dem Befehl die Gültigkeitsliste mit den Chiffre-Suites angezeigt, die von der Domäne verwendet werden wird.  Bei „false“ werden mit dem Befehl die Chiffre-Suites für die Informatica-Domäne so aktualisiert, dass die Gültigkeitsliste mit Chiffre-Suites verwendet wird. Standardwert ist „false“.
-cipherWhiteList -cwl	CipherSuiteName01,CiphersuiteName02, ...	Optional. Eine kommagetrennte Liste mit Chiffre-Suites, die Sie in die Gültigkeitsliste aufnehmen möchten. Verwenden Sie den vollständigen Registrierungsnamen der IANA TLS-Chiffre-Suites oder einen regulären Java-Ausdruck.  Diese Liste überschreibt die bisherige Whitelist. <b>Hinweis:</b> Die Liste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-cipherWhiteListFile -cwlf	whitelist_file_location	Optional. Absoluter Dateipfad und Dateiname einer Klartextdatei mit einer kommagetrennten Liste mit Chiffre-Suites, die Sie in die Gültigkeitsliste aufnehmen möchten.  Diese Liste überschreibt die bisherige Whitelist.  Verwenden Sie den vollständigen Registrierungsnamen der IANA TLS-Chiffre-Suites oder einen regulären Java-Ausdruck. <b>Hinweis:</b> Die Liste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-cipherBlackList -cbl	CipherSuiteName01,CiphersuiteName02, ...	Optional. Eine kommagetrennte Liste mit Chiffre-Suites, die Sie aus der Gültigkeitsliste entfernen möchten. Verwenden Sie den vollständigen Registrierungsnamen der IANA TLS-Chiffre-Suites oder einen regulären Java-Ausdruck.  Diese Liste überschreibt die bisherige Blacklist. <b>Hinweis:</b> Die Gültigkeitsliste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-cipherBlackListFile -cblf	blacklist_file_location	Optional. Absoluter Dateipfad und Dateiname einer Klartextdatei mit einer kommagetrennten Liste mit Chiffre-Suites, die Sie aus der Gültigkeitsliste entfernen möchten. Verwenden Sie den vollständigen Registrierungsnamen der IANA TLS-Chiffre-Suites oder einen regulären Java-Ausdruck.  Diese Liste überschreibt die bisherige Liste. <b>Hinweis:</b> Die Gültigkeitsliste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.

# updateDomainName

Ändert den Domänennamen in der Domänenkonfigurationsdatenbank.

Bevor Sie den Domänennamen aktualisieren, müssen Sie die Domäne, den standortspezifischen Schlüssel und die Keytab-Dateien sichern. Wenn das PowerCenter-Repository ein globales Repository enthält, müssen Sie die Registrierung aller lokalen Repositories über das globale Repository aufheben.

Um den Domänennamen zu aktualisieren, führen Sie den Befehl „infasetup updateDomainName“ von einem beliebigen Gateway-Knoten aus.

Nachdem Sie die Domäne aktualisiert haben, führen Sie die folgenden Schritte durch:

1. Führen Sie die Befehle „updateGatewayNode“ und „updateWorkerNode“ mit dem aktualisierten Domänennamen für alle Gateway- und Worker-Knoten aus.
2. Sie können das lokale Repository mit einem verbundenen globalen Repository mit dem Befehl „pmrep Register“ mit dem aktualisierten Domänennamen registrieren.
3. Sie können SPN und Keytab-Dateien mit dem aktualisierten Domänennamen für die Kerberos-Authentifizierung erstellen. Kopieren Sie die Keytab-Dateien in das Schlüsselverzeichnis. Sie können die ältere Standortschlüsseldatei weiter verwenden. Wenn Sie einen fehlenden oder fehlerhaften Standortschlüssel erneut generieren müssen, müssen Sie den älteren Domänennamen angeben.
4. Sie müssen die Informatica-Clients für die Verwendung des aktualisierten Domänennamens konfigurieren.

Für den Befehl „updateDomainName“ wird die folgende Syntax verwendet:

```
updateDomainName
-dn <domain_name>
```

In der folgenden Tabelle werden die *infasetup* Help-Option und das -Argument beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Ändert den Domänennamen. Domänennamen müssen zwischen 1 und 79 Zeichen umfassen und dürfen weder Leerzeichen noch die folgenden Zeichen enthalten: / * ? < >

# UpdateGatewayNode

Aktualisiert die Konnektivitätsinformationen für einen Gateway-Knoten auf dem aktuellen Computer. Führen Sie vor dem Aktualisieren des Gateway-Knotens den *infacmd isp ShutDownNode*-Befehl aus, um den Knoten herunterzufahren.

Der Befehl „UpdateGatewayNode“ verwendet die folgende Syntax:

```
UpdateGatewayNode
[<-DatabaseAddress|-da> database_hostname:database_port|<-DatabaseConnectionString|-cs>
database_connection_string]
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
[<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE|POSTGRESQL]
[<-DatabaseServiceName|-ds> database_service_name]
[<-DomainName|-dn> domain_name]
[<-NodeName|-nn> node_name]
[<-NodeAddress|-na> node_host:port]
```

```
[<-ServiceManagerPort|-sp> service_manager_port]
[<-EnableTLS|-tls> enable_tls]
[<-NodeKeystore|-nk> node_keystore_directory]
[<-NodeKeystorePass|-nkp> node_keystore_password]
[<-NodeTruststore|-nt> node_truststore_directory]
[<-NodeTruststorePass|-ntp> node_truststore_password]
[<-CipherWhiteList|-cwl> comma_separated_white_list_jsse_cipher_names]
[<-CipherBlackList|-cbl> comma_separated_black_list_jsse_cipher_names]
[<-CipherWhiteListFile|-cwlf>
absolute_filename_containing_comma_separated_white_list_jsse_cipher_names]
[<-CipherBlackListFile|-cbLf>
absolute_filename_containing_comma_separated_black_list_jsse_cipher_names]
[<-EnableKerberos|-krb> enable_kerberos]
[<-ServiceRealmName|-srn> realm_name_of_node_spn]
[<-UserRealmName|-urn> realm_name_of_user_spn]
[<-KeysDirectory|-kd> infa_keys_directory_location]
[<-EnableSaml|-saml> enable_saml]
[<-SamlTrustStoreDir|-std> saml_truststore_directory]
[<-SamlTrustStorePassword|-stp> saml_truststore_password]
[<-EnableSaml|-saml> enable_saml]
[<-SamlTrustStoreDir|-std> saml_truststore_directory]
[<-SamlTrustStorePassword|-stp> saml_truststore_password]
[<-SamlKeyStoreDir|-skd> saml_keystore_directory]
[<-SamlKeyStorePassword|-skp> saml_keystore_password]
[<-AdminconsolePort|-ap> admin_tool_port]
[<-HttpsPort|-hs> admin_tool_https_port]
[<-KeystoreFile|-kf> admin_tool_keystore_file_location]
[<-KeystorePass|-kp> admin_tool_keystore_password]
[<-LogServiceDirectory|-ld> log_service_directory]
[<-SystemLogDirectory|-sld> system_log_directory]
[<-ServerPort|-sv> server_shutdown_port]
[<-AdminconsoleShutdownPort|-asp> admin_tool_shutdown_port]
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for MSSQLServer only)]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
[<-TrustedConnection|-tc> trusted_connection (used for MSSQLServer only)]
[<-resetHostPort|-rst> resetHostPort]
```

In der folgenden Tabelle werden die Optionen und Argumente für „*infasetup* UpdateGatewayNode“ beschrieben:

Option	Beschreibung
-DatabaseAddress -da	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Name und Portnummer des Computers, auf dem die Konfigurationsdatenbank der Domäne gehostet wird.
-DatabaseConnectionString -cs	Erforderlich, wenn Sie die Optionen -DatabaseAddress (-da) und -DatabaseServiceName (-ds) nicht verwenden. Verbindungszeichenfolge, die zum Herstellen einer Verbindung zur Konfigurationsdatenbank der Domäne verwendet wird. Geben Sie den Namen des Datenbankhosts, -ports und -diensts als Teil der Verbindungszeichenfolge ein. Setzen Sie die Verbindungszeichenfolge in Anführungszeichen.
-DatabaseUserName -du	Erforderlich, wenn Sie die Option -TrustedConnection (-tc) nicht verwenden. Konto für die Datenbank, die die Domänenkonfigurationsinformationen enthält.
-DatabasePassword -dp	Passwort aus der Datenbank für die Domänenkonfiguration des Datenbankbenutzers. Wenn Sie diese Option weglassen, verwendet <i>infasetup</i> das in der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD angegebene Passwort. Wird in der Umgebungsvariable kein Wert angegeben, müssen Sie ein Passwort unter Verwendung dieser Option eingeben.

Option	Beschreibung
-DatabaseType -dt	Erforderlich. Typ der Datenbank, in der die Domänenkonfigurationsmetadaten gespeichert werden. Zu den Datenbanktypen gehören: <ul style="list-style-type: none"> <li>- db2</li> <li>- oracle</li> <li>- mssqlserver</li> <li>- sybase</li> <li>- postgresql</li> </ul>
-DatabaseServiceName -ds	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Der Name des Datenbankdiensts. Erforderlich für Oracle-, IBM DB2- und Microsoft SQL Server-Datenbanken. Geben Sie die SID für Oracle, den Dienstnamen für IBM DB2 oder den Datenbanknamen für Microsoft SQL Server ein.
-DomainName -dn	Optional. Name der Domäne.
-NodeName -nn	Optional. Name des Knotens. Knotennamen müssen zwischen 1 und 79 Zeichen umfassen und dürfen weder Leerzeichen noch die folgenden Zeichen enthalten: \ / * ? < > "
-NodeAddress -na	Optional. Hostname und Portnummer für den Computer, auf dem der Knoten gehostet wird. Wählen Sie eine verfügbare Portnummer aus.
-ServiceManagerPort -sp	Optional. Portnummer, die vom Dienstmanager verwendet wird, um auf eingehende Verbindungsanfragen zu reagieren.
-EnableTLS -tls	Optional. Konfiguriert die sichere Kommunikation für die Dienste in der Informatica-Domäne.  Wenn Sie die standardmäßigen, von Informatica bereitgestellten SSL-Zertifikate verwenden, müssen Sie die Schlüsselspeicher- und Truststore-Optionen nicht angeben. Wenn Sie das SSL-Zertifikat nicht verwenden, müssen Sie die Keystore- und Truststore-Optionen angeben. Gültige Werte sind „True“ oder „False“. Standardwert ist „False“. Wenn Sie die Option -tls ohne Wert angeben, verwendet die Informatica-Domäne die sichere Kommunikation zwischen Diensten.  Zum Aktivieren der sicheren Kommunikation für die verbundenen Dienste oder Webanwendungen, z. B. das Administrator Tool, das Analyst Tool oder den Webdienst-Hub, konfigurieren Sie die sichere Kommunikation separat innerhalb der Anwendungen.
-NodeKeystore -nk	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Verzeichnis, das die Schlüsselspeicherdateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS-Dateien (Java Keystore) vorliegen. Das Verzeichnis muss Schlüsselspeicherdateien in den Formaten PEM und JKS enthalten.  Die Schlüsselspeicherdateien müssen infa_keystore.jks und infa_keystore.pem lauten. Wenn die Schlüsselspeicherdatei, die Sie von der Zertifizierungsstelle erhalten, einen anderen Namen hat, müssen Sie sie in infa_keystore.jks und infa_keystore.pem umbenennen.  Sie müssen für alle Knoten in der Domäne dieselben Schlüsselspeicherzertifikate verwenden.

Option	Beschreibung
-NodeKeystorePass -nkp	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die Schlüsselspeicherdatei infa_keystore.jks.
-NodeTruststore -nt	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Verzeichnis, das die Truststore-Dateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS-Dateien (Java Keystore) vorliegen. Das Verzeichnis muss Truststore-Dateien in den Formaten PEM und JKS enthalten.  Die Truststore-Dateien müssen die Namen infa_truststore.jks und infa_truststore.pem aufweisen. Wenn die Truststore-Datei, die Sie von der Zertifizierungsstelle erhalten haben, einen anderen Namen aufweist, müssen Sie sie in infa_truststore.jks und infa_truststore.pem umbenennen.
-NodeTruststorePass -ntp	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die Datei infa_truststore.jks.
-CipherWhiteList -cwl	Optional. Eine kommagetrennte Liste mit JSSE-Chiffre-Suites, die zur Gültigkeitsliste hinzugefügt werden sollen. Diese Liste überschreibt die bisherige Whitelist. <b>Hinweis:</b> Die Liste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-CipherBlackList -cbl	Optional. Eine kommagetrennte Liste mit JSSE-Chiffre-Suites, die aus der Gültigkeitsliste entfernt werden sollen. Diese Liste überschreibt die bisherige Blacklist. <b>Hinweis:</b> Die Gültigkeitsliste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-CipherWhiteListFile -cwlf	Optional. Absoluter Dateiname der Klartextdatei, die eine kommagetrennte Liste mit Chiffre-Suites enthält, die der Gültigkeitsliste hinzugefügt werden sollen. Diese Liste überschreibt die bisherige Whitelist. <b>Hinweis:</b> Die Liste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-CipherBlackListFile -cblf	Optional. Absoluter Dateiname der Klartextdatei, die eine kommagetrennte Liste mit Chiffre-Suites enthält, die aus der Gültigkeitsliste entfernt werden sollen. Diese Liste überschreibt die bisherige Blacklist. <b>Hinweis:</b> Die Gültigkeitsliste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-EnableKerberos -krb	Optional. Konfiguriert die Informatica-Domäne zur Verwendung der Kerberos-Authentifizierung. Gültige Werte sind „True“ oder „False“.  Bei True verwendet die Domäne die Kerberos-Authentifizierung, dann können Sie den Authentifizierungsmodus später nicht ändern. Nachdem Sie die Kerberos-Authentifizierung aktiviert haben, können Sie sie nicht deaktivieren. Der Standardwert ist „false“.  Wenn Sie die Option -krb ohne einen Wert angeben, verwendet die Informatica-Domäne die Kerberos-Authentifizierung.

Option	Beschreibung
-ServiceRealmName -srn	<p>Optional. Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung.</p> <p>Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie den Namen des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird, getrennt durch Kommas ein. Beispiel: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Geben Sie beispielsweise folgenden Wert an, um alle Bereiche einzuschließen, die den Namen EAST.COMPANY.COM enthalten: *EAST.COMPANY.COM</p>
-UserRealmName -urn	<p>Optional. Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung.</p> <p>Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie den Namen des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird, getrennt durch Kommas ein. Beispiel: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Geben Sie beispielsweise folgenden Wert an, um alle Bereiche einzuschließen, die den Namen EAST.COMPANY.COM enthalten: *EAST.COMPANY.COM</p>
-KeysDirectory -kd	<p>Optional. Verzeichnis, in dem alle Schlüsseltabellendateien und der Verschlüsselungsschlüssel für die Informatica-Domäne gespeichert werden. Standardwert ist &lt;InformaticaInstallationDir&gt;/isp/config/keys.</p>
-EnableSaml -saml	<p>Optional. Aktiviert oder deaktiviert die SAML-Authentifizierung in der Informatica-Domäne.</p> <p>Legen Sie diesen Wert auf „true“ fest, um die SAML-Authentifizierung in der Informatica-Domäne zu aktivieren. Der Standardwert ist „false“.</p>
-SamlTrustStoreDir -std	<p>Optional. Das Verzeichnis mit der benutzerdefinierten Truststore-Datei, die für die Verwendung der SAML-Authentifizierung auf dem Gateway-Knoten erforderlich ist. Geben Sie nur das Verzeichnis an, nicht den vollständigen Pfad zur Datei.</p> <p>Der Informatica-Standard-Truststore wird verwendet, wenn kein Truststore angegeben ist.</p>
-SamlTrustStorePassword -stp	<p>Erforderlich, wenn Sie einen benutzerdefinierten Truststore für die SAML-Authentifizierung verwenden. Das Passwort für den benutzerdefinierten Truststore.</p>
-SamlKeyStoreDir -skd	<p>Optional. Das Verzeichnis mit der benutzerdefinierten Truststore-Datei, die für die Verwendung der SAML-Authentifizierung auf dem Gateway-Knoten erforderlich ist. Geben Sie nur das Verzeichnis an, nicht den vollständigen Pfad zur Datei.</p>
-SamlKeyStorePassword -skp	<p>Erforderlich, wenn Sie einen benutzerdefinierten Schlüsselspeicher für die SAML-Authentifizierung verwenden. Passwort für den SAML-Schlüsselspeicher. *</p>
-AdminconsolePort -ap	<p>Optional. Port für den Zugriff auf Informatica Administrator.</p>

Option	Beschreibung
-HttpsPort -hs	Optional. Portnummer zum Sichern der Verbindung zum Administrator Tool. Geben Sie diese Portnummer an, wenn Sie HTTPS für einen Knoten konfigurieren möchten. Zum Deaktivieren von HTTPS-Unterstützung für einen Knoten setzen Sie diese Portnummer auf Null.
-KeystoreFile -kf	Optional. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die bei Verwendung des SSL-Protokolls erforderlich sind
-KeystorePass -kp	Optional. Ein Klartext-Passwort für die Schlüsselspeicherdatei. Sie können ein Passwort mit der Option -kp oder der Umgebungsvariable INFA_PASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -kp festgelegte Passwort Vorrang.
-LogServiceDirectory -ld	Optional. Freigegebener Verzeichnispfad, der vom Protokollmanager zum Speichern von Protokollereignisdateien verwendet wird. Stellen Sie sicher, dass -ld nicht übereinstimmt oder den angegebenen Wert für -sld enthält.
-SystemLogDirectory -sld	Optional. Verzeichnispfad zum Speichern von Systemprotokolldateien. Stellen Sie sicher, dass -ld nicht übereinstimmt oder den angegebenen Wert für -sld enthält. Standard ist <INFA_home>/logs.
-ServerPort -sv	Optional. Vom Dienstmanager verwendete TCP/IP-Portnummer. Der Dienstmanager verwaltet Befehle zum Herunterfahren aus PowerCenter-Komponenten auf diesem Port. Legen Sie diese Portnummer fest, wenn sich auf einem Computer mehrere Knoten befinden oder die Standardportnummer verwendet wird. Standardwert ist 8005.
-AdminconsoleShutdownPort -asp	Optional. Portnummer, die das Herunterfahren für Informatica Administrator steuert.
-Tablespace -ts	Erforderlich für eine IBM DB2-Datenbank. Name des Tablespace, in dem sich die Datenbanktabellen für die Domänenkonfiguration befinden.
-SchemaName -sc	Optional. Name des Microsoft SQL Server-Schemas. Geben Sie einen Schemanamen ein, wenn Sie nicht das Standardschema verwenden.
-DatabaseTlsEnabled -dbtls	Optional. Gibt an, ob die Informatica-Domänendatenbank mit TLS und SSL sicher ist. Setzen Sie diese Option für die sichere Datenbank auf True. Standardwert ist „False“. Wenn die Option -dbtls ohne Wert angegeben wird, verwendet die Informatica-Domäne die sichere Kommunikation mit der Informatica-Domänendatenbank.
-DatabaseTruststorePassword -dbtp	Optional. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.
-TrustedConnection -tc	Optional. Stellen Sie eine Verbindung zur Microsoft SQL Server-Datenbank über eine vertrauenswürdige Verbindung her. Die vertrauenswürdige Authentifizierung verwendet die Windows-Sicherheitsanmeldedaten des aktuellen Benutzers, um eine Verbindung zu Microsoft SQL Server herzustellen.
-resetHostPort -rst	Erforderlich, wenn Sie die Option NodeAddress oder ServiceManager angeben. Setzt die Portnummer des Hosts zurück.



Option	Beschreibung
-DatabaseTruststoreLocation -dbtl	Optional. Pfad und Dateiname der Truststore-Datei für den Gateway-Knoten.
* Hinweis: Wenn Sie derzeit Skripts ausführen, die diesen Befehl verwenden, um einen benutzerdefinierten Schlüsselspeicher für die SAML-Authentifizierung zu aktivieren, müssen Sie diese aktualisieren, um diese Option aufzunehmen.	

## UpdateKerberosAdminUser

Aktualisiert den Kerberos-Standardadministrator im Domänen-Repository.

Der Befehl `UpdateKerberosAdminUser` verwendet die folgende Syntax:

```
UpdateKerberosAdminUser
<-KerberosAdminName|-kan> kerberos_admin_name
```

In der folgenden Tabelle werden die *infasetup* `UpdateKerberosAdminUser`-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-KerberosAdminName -kan	kerberos_admin_name	Erforderlich. Name des Benutzers, der als Standardadministrator ausgewählt werden soll. Wenn die Domäne einen einzelnen Kerberos-Bereich zum Authentifizieren von Benutzern verwendet, geben Sie den SAM-Kontonamen an. Wenn die Domäne die bereichsübergreifende Kerberos-Authentifizierung verwendet, geben Sie den vollqualifizierten Benutzerprinzipalnamen, einschließlich des Bereichsnamens, an. Beispiel: sysadmin@COMPANY.COM

## UpdateKerberosConfig

Verwenden Sie den Befehl „`UpdateKerberosConfig`“, um den Bereichsnamen oder den Dienst-Bereichsnamen in der Informatica-Konfiguration zu korrigieren. Sie können den Benutzerbereich ändern, zu dem die Informatica-Domänenbenutzer gehören. Sie können den Dienstbereich ändern, zu dem die Informatica-Domänendienste gehören.

**Hinweis:** Dieser Befehl ändert nicht die Kerberos-Konfiguration. Sie können mit diesem Befehl keine Benutzer von einem Benutzer- oder Dienstbereich in einen anderen Benutzer- oder Dienstbereich migrieren.

Der Befehl „`UpdateKerberosConfig`“ verwendet die folgende Syntax:

```
UpdateKerberosConfig
[<-ServiceRealmName|-srn> realm_name_of_node_spn]
```

[<-UserRealmName|-urn> realm\_name\_of\_user\_spn]

In der folgenden Tabelle werden Optionen und Argumente für „infasetup UpdateKerberosConfig“ beschrieben:

Option	Argument	Beschreibung
-ServiceRealmName -srn	realm_name_of_node_spn	<p>Optional. Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung.</p> <p>Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie den Namen des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird, getrennt durch Kommas ein. Beispiel:</p> <p>COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Geben Sie beispielsweise folgenden Wert an, um alle Bereiche einzuschließen, die den Namen EAST.COMPANY.COM enthalten:</p> <p>*EAST.COMPANY.COM</p>
-UserRealmName -urn	realm_name_of_user_spn	<p>Optional. Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung.</p> <p>Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie den Namen des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird, getrennt durch Kommas ein. Beispiel:</p> <p>COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Geben Sie beispielsweise folgenden Wert an, um alle Bereiche einzuschließen, die den Namen EAST.COMPANY.COM enthalten:</p> <p>*EAST.COMPANY.COM</p>

## updateMitKerberosLinkage

Konfiguriert benutzerdefinierte Datenbank-Clients und die Informatica-Domäne zur Verwendung der angegebenen benutzerdefinierten Kerberos-Bibliotheken statt der von Informatica verwendeten Standardbibliotheken.

Gehen Sie zur Verwendung benutzerdefinierter Kerberos-Bibliotheken folgendermaßen vor:

1. Kopieren Sie die zu verwendenden benutzerdefinierten Kerberos-Bibliotheken auf alle Knoten oder in einen Speicherort, auf den alle Knoten in der Informatica-Domäne zugreifen können.

2. Fahren Sie die Domäne herunter.
3. Führen Sie den Befehl „infasetup updateMitKerberosLinkage“ auf allen Knoten in der Domäne aus.
4. Starten Sie die Domäne nach Ausführung des Befehls auf allen Knoten in der Domäne.

Der Befehl „updateMitKerberosLinkage“ verwendet die folgende Syntax:

```
updateMitKerberosLinkage
<-useKeberos|-krb> true|false
[<-mitKerberosDirectory|-mkd> kerberos_library_directory]
```

In der folgenden Tabelle werden die Optionen und Argumente des Befehls „infasetup updateMitKerberosLinkage“ beschrieben:

Option	Argument	Beschreibung
-useKeberos -krb	true false	<p>Erforderlich. Boolescher Wert. Legen Sie diesen Wert auf TRUE fest, wenn die Informatica-Domäne Kerberos-Authentifizierung verwendet. Wenn dieser Wert auf TRUE festgelegt ist, verarbeitet Informatica Kerberos-Aufrufe mit den Kerberos-Standardbibliotheken oder den Bibliotheken in dem mit der Option -mkd angegebenen Verzeichnis.</p> <p>Legen Sie diesen Wert auf FALSE fest, wenn Kerberos in der Informatica-Domäne nicht verwendet wird. Wenn dieser Wert auf FALSE festgelegt ist, lädt Informatica keine Kerberos-Bibliotheken. Drittanbieter-Clients, wie z. B. Datenbank-Clients, führen Kerberos-Aufrufe mit den Bibliotheken durch, die in dem mit der Option -mkd festgelegten Verzeichnis angegeben sind.</p>
-mitKerberosDirectory -mkd	kerberos_library_directory_node_spn	<p>Optional. Das Verzeichnis, das die benutzerdefinierten MIT-Kerberos-Bibliotheken enthält. Das Verzeichnis muss die Bibliotheksdateien enthalten. Symbolische Verknüpfungen können nicht verwendet werden.</p> <p>Wenn die Option -krb auf TRUE festgelegt ist, stellen Sie sicher, dass die zu verwendenden benutzerdefinierten Kerberos-Bibliotheken dieselbe Versionsnummer aufweisen wie die von Informatica standardmäßig verwendeten Kerberos-Bibliotheken.</p> <p>Liegen mehrere Versionen derselben Bibliothek vor, müssen alle Versionen die gleiche Größe und die gleiche Prüfsumme aufweisen. Wenn das Verzeichnis beispielsweise zwei Versionen von libkrb5 (libkr5.so.3 und libkrb5.so) enthält, sollten beide Bibliotheken dieselbe Dateigröße und denselben Prüfsummenwert aufweisen.</p> <p>Wenn das angegebene Verzeichnis leer ist, entfernt der Befehl alle benutzerdefinierten Kerberos-Bibliotheken aus der Informatica-Domäne.</p>

# UpdatePasswordComplexityConfig

Aktualisiert die Konfiguration der Passwortkomplexität für die Domäne.

Der Befehl „infasetup UpdatePasswordComplexityConfig“ verwendet folgende Syntax:

```
UpdatePasswordComplexityConfig
<-EnablePasswordComplexity|-pc> enable_password_complexity
```

In der folgenden Tabelle werden die Optionen und Argumente für infasetup UpdatePasswordComplexityConfig beschrieben:

Option	Argument	Beschreibung
-EnablePasswordComplexity -pc	enable_password_complexity	<p>Optional. Aktiviert die Passwortkomplexität, um die Passwortstärke zu validieren. Diese Option ist standardmäßig deaktiviert.</p> <p>Wenn Sie für ein natives Benutzerkonto die Passwortkomplexität aktivieren, beachten Sie beim Erstellen oder Ändern eines Passworts Folgendes:</p> <ul style="list-style-type: none"><li>- Das Passwort muss aus mindestens acht Zeichen bestehen.</li><li>- Es muss mindestens einen Buchstaben, eine Zahl und ein nicht alphanumerisches Zeichen enthalten, z. B.:</li></ul> <pre>! \ " # \$ % &amp; ' ( ) * + , - . / : ; &lt; = &gt; ? @ [ ] ^ _ ` {   } ~</pre> <p>Manche Sonderzeichen in Passwörtern können von der Shell anders interpretiert werden. Beispielsweise wird \$ als Variable interpretiert. Setzen Sie in diesem Fall ein Escape-Zeichen vor das betreffende Sonderzeichen.</p>

# updateDomainSamlConfig

Aktiviert oder deaktiviert die SAML-Authentifizierung (Secure Assertion Markup Language) für Informatica-Webanwendungen in einer Informatica-Domäne. Sie können den Befehl auch zum Aktualisieren der URL des Identitätsanbieters und zum Angeben des zulässigen zeitlichen Unterschieds zwischen der Systemuhr des Identitätsanbieter-Hosts und der Systemuhr des Master-Gateway-Knotens verwenden.

Führen Sie den Befehl auf jedem Gateway-Knoten innerhalb der Informatica-Domäne aus. Fahren Sie die Domäne vor dem Ausführen des Befehls herunter.

Der Befehl „infasetup updateDomainSamlConfig“ verwendet folgende Syntax:

```
updateDomainSamlConfig
[<-EnableSaml|-saml> enable_saml]
[<-IdpUrl|-iu> idp_url]
[<-ServiceProviderId|-spid> service_provider_id]
[<-ClockSkewTolerance|-cst> clock_skew_tolerance_in_seconds]
[<-SamlAssertionSigned|-sas> sign_saml_assertion]
[<-AssertionSigningCertificateAlias|-asca> idp_assertion_signing_certificate_alias]
[<-AuthnContextComparsion|-acc> saml_requested_authn_context_comparsion_type]
[<-AuthnContextClassRef|-accr> saml_requested_authn_context_class_reference]
[<-SignSamlRequest|-ssr> sign_saml_request]
[<-RequestSigningPrivateKeyAlias|-rspa> saml_request_signing_private_key_alias]
[<-RequestSigningPrivateKeyPassword|-rspp> saml_request_signing_private_key_password]
```

```
[<-RequestSigningAlgorithm|-rsa> saml_request_signing_algorithm]
[<-SamlResponseSigned|-srs> saml_response_signed]
[<-ResponseSigningCertificateAlias|-rsca> idp_response_signing_certificate_alias]
[<-SamlAssertionEncrypted|-sae> saml_assertion_encrypted]
[<-EncryptedAssertionPrivateKeyAlias|-eapa> saml_encrypt_assertion_private_key_alias]
[<-EncryptedAssertionPrivateKeyPassword|-eapp>
saml_encrypt_assertion_private_key_password]
```

In der folgenden Tabelle werden die Optionen und Argumente des Befehls „infasetup updateDomainSamlConfig“ beschrieben:

Option	Beschreibung
-EnableSaml -saml	Optional. Aktiviert oder deaktiviert die SAML-Authentifizierung in der Informatica-Domäne. Legen Sie diesen Wert auf „true“ fest, um die SAML-Authentifizierung in der Informatica-Domäne zu aktivieren. Der Standardwert ist „false“.
-idpUrl -iu	Erforderlich, wenn die Option -saml auf TRUE festgelegt ist. Geben Sie die URL des Identitäts-Providers für die Domäne an. Sie müssen die vollständige URL-Zeichenfolge angeben.
-ServiceProviderId -spid	Optional. Der Vertrauensstellungsname der vertrauenswürdigen Partei oder die Kennung des Diensteanbieters für die Domäne, wie im Identitätsanbieter definiert. Wenn Sie „Informatica“ als Vertrauensstellungsname der vertrauenswürdigen Partei in AD FS angegeben haben, müssen Sie keinen Wert angeben.
-ClockSkewTolerance -cst	Optional. Der zulässige zeitliche Unterschied zwischen der Systemuhr des Identitätsanbieter-Hosts und der Systemuhr auf dem Master-Gateway-Knoten. Die Lebensdauer von SAML-Token, die vom Identitätsanbieter ausgegeben werden, wird entsprechend der Systemuhr des Identitätsanbieter-Hosts festgelegt. Die Lebensdauer eines von Identitätsanbieter ausgegebenen SAML-Tokens ist gültig, wenn die im Token festgelegte Startzeit oder Endzeit nicht mehr als die angegebene Anzahl an Sekunden von der Systemuhr auf dem Master-Gateway-Knoten abweicht. Die Werte müssen zwischen 0 und 600 Sekunden liegen. Standardwert ist 120 Sekunden.
-SamlAssertionSigned -sas	Optional. Setzen Sie den Parameter auf TRUE, um das Signieren von Assertionen durch den Identitätsanbieter zu aktivieren. Standardwert ist FALSE.
-AssertionSigningCertificateAlias -asca	Erforderlich, wenn SamlAssertionSigned auf TRUE gesetzt ist. Der Aliasname, der beim Importieren des Assertionssignaturzertifikats des Identitätsanbieters in die für die SAML-Authentifizierung verwendete Truststore-Datei angegeben wird.

Option	Beschreibung
-AuthnContextComparsion -accr	Gibt die Vergleichsmethode an, mit der die angeforderte Berechtigungserklärung ausgewertet wird. Eine der folgenden Optionen: <ul style="list-style-type: none"> <li>- MINIMUM. Der Authentifizierungskontext in der Authentifizierungsanweisung muss genau mit mindestens einem der angegebenen Authentifizierungskontexte übereinstimmen.</li> <li>- MAXIMUM. Der Authentifizierungskontext in der Authentifizierungsanweisung muss mindestens so stark (wie vom Antwortenden angenommen) sein wie einer der angegebenen Authentifizierungskontexte.</li> <li>- BETTER. Der Authentifizierungskontext in der Authentifizierungsanweisung muss stärker (wie vom Antwortenden angenommen) sein wie einer der angegebenen Authentifizierungskontexte.</li> <li>- EXACT. Der Authentifizierungskontext in der Authentifizierungsanweisung muss so stark wie möglich (wie vom Antwortenden angenommen) sein, ohne die Stärke von mindestens einem der angegebenen Authentifizierungskontexte zu überschreiten.</li> </ul> Der Standardwert ist EXACT.
-AuthnContextClassRef -accr	Die Klasse des Authentifizierungskontexts. Eine der folgenden Optionen: <ul style="list-style-type: none"> <li>- PASSWORD</li> <li>- PASSWORDPROTECTEDTRANSPORT</li> </ul>
-SignSamlRequest -ssr	Setzen Sie den Parameter auf „True“, um die Anforderungssignierung zu aktivieren. Der Standardwert ist FALSE.
-RequestSigningPrivateKeyAlias -rspa	Erforderlich, wenn Sie die Signieranforderung aktivieren. Aliasname des privaten Schlüssels, mit dem Informatica die Anforderung signiert. Dieser private Schlüssel befindet sich im Schlüsselspeicher des Gateway-Knotens. Der entsprechende öffentliche Schlüssel (normalerweise ein Zertifikat) sollte in den Identitätsanbieter importiert werden.
-RequestSigningPrivateKeyPassword -rspp	Klartext-Passwort des privaten Schlüssels, mit dem Informatica die Anforderung signiert. Standard ist das Passwort des privaten Schlüssels, der sich in der Keystore-Datei <Informatica-Startseite>\services\shared\security\infa_keystore.jks mit dem Alias „Informatica LLC“ befindet.
-RequestSigningAlgorithm -rsa	Erforderlich, wenn Sie die Signieranforderung aktivieren. Algorithmus zum Signieren der Anforderung. Eine der folgenden Optionen: <ul style="list-style-type: none"> <li>- RSA_SHA256</li> <li>- DSA_SHA1</li> <li>- DSA_SHA256</li> <li>- RSA_SHA1</li> <li>- RSA_SHA224</li> <li>- RSA_SHA384</li> <li>- RSA_SHA512</li> <li>- ECDSA_SHA1</li> <li>- ECDSA_SHA224</li> <li>- ECDSA_SHA256</li> <li>- ECDSA_SHA384</li> <li>- ECDSA_SHA512</li> <li>- RIPEMD160</li> <li>- RSA_MD5</li> </ul>

Option	Beschreibung
-SamlResponseSigned -srs	Setzen Sie den Parameter auf „True“, um anzugeben, ob der IDP die SAML-Antwort signiert. <b>Hinweis:</b> Bei der Einstellung TRUE muss der IDP-Administrator den Identifizierungsanbieter so konfigurieren, dass die Antwort signiert wird. Der Standardwert ist FALSE.
-ResponseSigningCertificateAlias -rsca	Erforderlich, wenn Sie die signierte Antwort aktivieren. Aliasname des Zertifikats im SAML-Truststore des Gateway-Knotens, mit dem die Signatur überprüft werden soll.
-SamlAssertionEncrypted -sae	Setzen Sie den Parameter auf „True“, um anzugeben, ob der IDP die Assertion signiert. <b>Hinweis:</b> Bei der Einstellung TRUE muss der IDP-Administrator den Identifizierungsanbieter so konfigurieren, dass die Assertion verschlüsselt wird. Der Standardwert ist FALSE.
-EncryptedAssertionPrivateKeyAlias -espa	Aliasname des privaten Schlüssels im SAML-Schlüsselspeicher des Gateway-Knotens. Der private Schlüssel wird zum Verschlüsseln der Assertion verwendet. Der IDP-Administrator muss den entsprechenden öffentlichen Schlüssel (normalerweise ein Zertifikat) importieren.
-EncryptedAssertionPrivateKeyPassword -espp	Klartext-Passwort. Standard ist das Passwort des privaten Schlüssels, der sich in der Keystore-Datei <Informatica-Startseite>\services\shared\security\infa_keystore.jks mit dem Alias „Informatica LLC“ befindet.

## UpdateWorkerNode

Aktualisiert die Konnektivitätsinformationen für einen Arbeitsknoten auf dem aktuellen Computer. Führen Sie vor dem Aktualisieren des Arbeitsknotens den `infacmd isp ShutDownNode`-Befehl aus, um den Knoten herunterzufahren.

Der Befehl „UpdateWorkerNode“ verwendet die folgende Syntax:

```
UpdateWorkerNode
[<-DomainName|-dn> domain_name]
[<-NodeName|-nn> node_name]
[<-NodeAddress|-na> node_host:port]
[<-ServiceManagerPort|-sp> service_manager_port]
[<-EnableTLS|-tls> enable_tls]
[<-NodeKeystore|-nk> node_keystore_directory]
[<-NodeKeystorePass|-nkp> node_keystore_password]
[<-NodeTruststore|-nt> node_truststore_directory]
[<-NodeTruststorePass|-ntp> node_truststore_password]
[<-CipherWhiteList|-cwl> comma_separated_white_list_jsse_cipher_names]
[<-CipherBlackList|-cbl> comma_separated_black_list_jsse_cipher_names]
[<-CipherWhiteListFile|-cwlf>
absolute_filename_containing_comma_separated_white_list_jsse_cipher_names]
[<-CipherBlackListFile|-cblf>
absolute_filename_containing_comma_separated_black_list_jsse_cipher_names]
[<-EnableKerberos|-krb> enable_kerberos]
[<-ServiceRealmName|-srn> realm_name_of_node_spn]
[<-UserRealmName|-urn> realm_name_of_user_spn]
[<-KeysDirectory|-kd> Infa_keys_directory_location]
[<-HttpsPort|-hs> admin_tool_https_port]
```

```
[<-KeystoreFile|-kf> admin_tool_keystore_file_location]
[<-KeystorePass|-kp> admin_tool_keystore_password]
[<-GatewayAddress|-dg> domain_gateway_host:port]
[<-UserName|-un> user_name]
[<-SecurityDomain|-sdn> security_domain]
[<-Password|-pd> password]
[<-ServerPort|-sv> server_shutdown_port]
[<-resetHostPort|-rst> resetHostPort]
[<-SystemLogDirectory|-sld> system_log_directory]
[<-EnableSaml|-saml> enable_saml]
[<-SamlKeyStoreDir|-skd> saml_keystore_directory]
[<-SamlKeyStorePassword|-skp> saml_keystore_password]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infasetup UpdateWorkerNode“ beschrieben:

Option	Beschreibung
-DomainName -dn	Optional. Name der Domäne.
-NodeName -nn	Optional. Name des Knotens. Knotennamen müssen zwischen 1 und 79 Zeichen umfassen und dürfen weder Leerzeichen noch die folgenden Zeichen enthalten: \ / * ? < > "
-NodeAddress -na	Optional. Hostname und Portnummer für den Computer, auf dem der Knoten gehostet wird. Wählen Sie eine verfügbare Portnummer aus.
-ServiceManagerPort -sp	Optional. Portnummer, die vom Dienstmanager verwendet wird, um auf eingehende Verbindungsanfragen zu reagieren.
-EnableTLS -tls	Optional. Konfiguriert die sichere Kommunikation für die Dienste in der Informatica-Domäne.  Wenn Sie die standardmäßigen, von Informatica bereitgestellten SSL-Zertifikate verwenden, müssen Sie die Schlüsselspeicher- und Truststore-Optionen nicht angeben. Wenn Sie das SSL-Zertifikat nicht verwenden, müssen Sie die Keystore- und Truststore-Optionen angeben. Gültige Werte sind „True“ oder „False“. Standardwert ist „False“. Wenn Sie die Option -tls ohne Wert angeben, verwendet die Informatica-Domäne die sichere Kommunikation zwischen Diensten.  Zum Aktivieren der sicheren Kommunikation für die verbundenen Dienste oder Webanwendungen, z. B. das Administrator Tool, das Analyst Tool oder den Webdienst-Hub, konfigurieren Sie die sichere Kommunikation separat innerhalb der Anwendungen.
-NodeKeystore- -nk	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Verzeichnis, das die Schlüsselspeicherdateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS-Dateien (Java Keystore) vorliegen. Das Verzeichnis muss Schlüsselspeicherdateien in den Formaten PEM und JKS enthalten.  Die Schlüsselspeicherdateien müssen infa_keystore.jks und infa_keystore.pem lauten. Wenn die Schlüsselspeicherdatei, die Sie von der Zertifizierungsstelle erhalten, einen anderen Namen hat, müssen Sie sie in infa_keystore.jks und infa_keystore.pem umbenennen.  Sie müssen für alle Knoten in der Domäne dieselben Schlüsselspeicherzertifikate verwenden.
-NodeKeystorePass -nkp	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die Schlüsselspeicherdatei infa_keystore.jks.



Option	Beschreibung
-NodeTruststore -nt	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Verzeichnis, das die Truststore-Dateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS-Dateien (Java Keystore) vorliegen. Das Verzeichnis muss Truststore-Dateien in den Formaten PEM und JKS enthalten.  Die Truststore-Dateien müssen die Namen infa_truststore.jks und infa_truststore.pem aufweisen. Wenn die Truststore-Datei, die Sie von der Zertifizierungsstelle erhalten haben, einen anderen Namen aufweist, müssen Sie sie in infa_truststore.jks und infa_truststore.pem umbenennen.
-NodeTruststorePass -ntp	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die Datei infa_truststore.jks.
-CipherWhiteList -cwl	Optional. Eine kommagetrennte Liste mit JSSE-Chiffre-Suites, die zur Gültigkeitsliste hinzugefügt werden sollen. <b>Hinweis:</b> Die Liste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-CipherBlackList -cbl	Optional. Eine kommagetrennte Liste mit JSSE-Chiffre-Suites, die aus der Gültigkeitsliste entfernt werden sollen. <b>Hinweis:</b> Die Gültigkeitsliste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-CipherWhiteListFile -cwlF	Optional. Absoluter Dateiname der Klartextdatei, die eine kommagetrennte Liste mit Chiffre-Suites enthält, die der Gültigkeitsliste hinzugefügt werden sollen. <b>Hinweis:</b> Die Liste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-CipherBlackListFile -cblF	Optional. Absoluter Dateiname der Klartextdatei, die eine kommagetrennte Liste mit Chiffre-Suites enthält, die aus der Gültigkeitsliste entfernt werden sollen. <b>Hinweis:</b> Die Gültigkeitsliste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-EnableKerberos -krb	Optional. Konfiguriert die Informatica-Domäne zur Verwendung der Kerberos-Authentifizierung. Gültige Werte sind „True“ oder „False“. Bei True verwendet die Domäne die Kerberos-Authentifizierung, dann können Sie den Authentifizierungsmodus später nicht ändern. Nachdem Sie die Kerberos-Authentifizierung aktiviert haben, können Sie sie nicht mehr deaktivieren.  Standardwert ist „False“. Wenn Sie die Option -krb ohne einen Wert angeben, verwendet die Informatica-Domäne die Kerberos-Authentifizierung.
-ServiceRealmName -srn	Optional. Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung.  Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie den Namen des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird, getrennt durch Kommas ein. Beispiel: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM  Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Geben Sie beispielsweise folgenden Wert an, um alle Bereiche einzuschließen, die den Namen EAST.COMPANY.COM enthalten: *EAST.COMPANY.COM

Option	Beschreibung
-UserRealmName -urn	<p>Optional. Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung.</p> <p>Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie den Namen des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird, getrennt durch Kommas ein. Beispiel: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Geben Sie beispielsweise folgenden Wert an, um alle Bereiche einzuschließen, die den Namen EAST.COMPANY.COM enthalten: *EAST.COMPANY.COM</p>
-KeysDirectory -kd	Optional. Verzeichnis, in dem alle Schlüsseltabellendateien und der Verschlüsselungsschlüssel für die Informatica-Domäne gespeichert werden. Standardwert ist <Informatica-Installationsverzeichnis>/isp/config/keys.
-HttpsPort -hs	Optional. Portnummer zum Sichern der Verbindung zum Administrator Tool. Geben Sie diese Portnummer an, wenn Sie HTTPS für einen Knoten konfigurieren möchten.
-KeystoreFile -kf	Optional. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die bei Verwendung des SSL-Protokolls erforderlich sind
-KeystorePass -kp	Optional. Ein Volltext-Passwort für die Schlüsselspeicherdatei. Sie können ein Passwort mit der Option -kp oder der Umgebungsvariable INFA_PASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -kp festgelegte Passwort Vorrang.
-GatewayAddress -dg	Erforderlich. Name und Portnummer des Gateway-Hostcomputers.
-UserName -un	<p>Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.</p> <p>Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.</p>
-SecurityDomain -sdn	<p>Name der Sicherheitsdomäne, die Sie erstellen möchten und zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänenamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Sie können einen Wert für -sdn angeben oder den Standardwert basierend auf dem Authentifizierungsmodus verwenden:</p> <ul style="list-style-type: none"> <li>- Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Standardwert ist „Nativ“. Zum Arbeiten mit der LDAP-Authentifizierung müssen Sie den Wert für -sdn angeben.</li> <li>- Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Standardwert ist „Native“ für native Authentifizierung. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</li> </ul>

Option	Beschreibung
-Password -pd	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-MinProcessPort -mi	Erforderlich. Kleinste Portnummer für die Anwendungsdienstprozesse, die auf dem Knoten ausgeführt werden.
-MaxProcessPort -ma	Erforderlich. Größte Portnummer für die Anwendungsdienstprozesse, die auf dem Knoten ausgeführt werden.
-ServerPort -sv	Optional. Vom Dienstmanager verwendete TCP/IP-Portnummer. Der Dienstmanager verwaltet Befehle zum Herunterfahren aus Domänenkomponenten auf diesem Port. Legen Sie diese Portnummer fest, wenn sich auf einem Computer mehrere Knoten befinden oder die Standardportnummer verwendet wird. Als Standardwert fungiert die Portnummer des Knotens plus eins.
-BackupDirectory -bd	Optional. Verzeichnis zum Speichern der Repository-Backup-Dateien. Der Zugriff auf das Verzeichnis muss über den Knoten möglich sein.
-ErrorLogLevel -el	Optional. Schweregradstufe für Protokollereignisse im Domänenprotokoll. Standardwert ist „info“.
-ResourceFile -rf	Erforderlich. Datei, die eine Liste der verfügbaren Ressourcen für den Knoten enthält. Verwenden Sie die Datei „nodeoptions.xml“, die sich an folgendem Speicherort befindet: <Informatica installation directory>/isp/bin
-EnableSaml -saml	Optional. Aktiviert oder deaktiviert die SAML-Authentifizierung in der Informatica-Domäne. Legen Sie diesen Wert auf „true“ fest, um die SAML-Authentifizierung in der Informatica-Domäne zu aktivieren. Der Standardwert ist „false“.
-SamlKeyStoreDir -skd	Optional. Das Verzeichnis mit der benutzerdefinierten Truststore-Datei, die für die Verwendung der SAML-Authentifizierung auf dem Gateway-Knoten erforderlich ist. Geben Sie nur das Verzeichnis an, nicht den vollständigen Pfad zur Datei.
-SamlKeyStorePassword -skp	Erforderlich, wenn Sie einen benutzerdefinierten Schlüsselspeicher für die SAML-Authentifizierung verwenden. Passwort für den SAML-Schlüsselspeicher. *
-GatewayAddress -dg	Erforderlich. Name und Portnummer des Gateway-Hostcomputers.
-UserName -un	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.  Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Beschreibung
-SecurityDomain -sdn	<p>Name der Sicherheitsdomäne, die Sie erstellen möchten und zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.</p> <p>Sie können einen Wert für -sdn angeben oder den Standardwert basierend auf dem Authentifizierungsmodus verwenden:</p> <ul style="list-style-type: none"> <li>- Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Standardwert ist „Nativ“. Zum Arbeiten mit der LDAP-Authentifizierung müssen Sie den Wert für -sdn angeben.</li> <li>- Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Standardwert ist „Native“ für native Authentifizierung. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.</li> </ul>
-Password -pd	<p>Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.</p>
-ServerPort -sv	<p>Optional. Vom Dienstmanager verwendete TCP/IP-Portnummer. Der Dienstmanager verwaltet Befehle zum Herunterfahren aus PowerCenter-Komponenten auf diesem Port. Legen Sie diese Portnummer fest, wenn sich auf einem Computer mehrere Knoten befinden oder die Standardportnummer verwendet wird.</p>
-resetHostPort -rst	<p>Erforderlich, wenn Sie die Option NodeAddress oder ServiceManager angeben. Setzt die Portnummer des Hosts zurück.</p>
-SystemLogDirectory -sld	<p>Optional. Verzeichnispfad zum Speichern von Systemprotokolldateien. Standard ist &lt;INFA_home&gt;/logs.</p>
<p>* Hinweis: Wenn Sie derzeit Skripts ausführen, die diesen Befehl verwenden, um einen benutzerdefinierten Schlüsselspeicher für die SAML-Authentifizierung zu aktivieren, müssen Sie diese aktualisieren, um diese Option aufzunehmen.</p>	

## upgradeDomainMetadata

Aktualisiert Metadaten für die Domäne. Führen Sie vor dem Aktualisieren der Domäne den Befehl „infacmd isp ShutDownNode“ aus, um den Knoten herunterzufahren.

Der Befehl „upgradeDomainMetadata“ verwendet die folgende Syntax:

```
upgradeDomainMetadata
<-PreviousInfaHome|-ph> previous_infa_home
<<-DatabaseAddress|-da> database_hostname:database_port|<-DatabaseConnectionString|-cs>
database_connection_string>
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE|POSTGRESQL
[<-DatabaseServiceName|-ds> database_service_name]
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for MSSQLServer and PostgreSQL only)]
```

```
[<-TrustedConnection|-tc> trusted_connection (used for MSSQLServer only)]
[<-KeysDirectory|-kd> Infa_secrets_directory_location]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
[<-SingletonServiceParameters|-ssp> option_name=value ...(SystemServicesFolderName,
SchedulerService, ResourceManager, EmailService)]
```

In der folgenden Tabelle werden die *infasetup*-Optionen und -Argumente für „upgradeDomainMetadata“ beschrieben:

Option	Beschreibung
-PreviousInfaHome -ph	Erforderlich. Pfad zum vorherigen Informatica-Startverzeichnis.
-DatabaseAddress -da	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Name und Portnummer des Computers, auf dem die Konfigurationsdatenbank der Domäne gehostet wird.
-DatabaseUserName -du	Erforderlich, wenn Sie die Option -TrustedConnection (-tc) nicht verwenden. Konto für die Datenbank, die die Domänenkonfigurationsinformationen enthält.
-DatabasePassword -dp	Passwort aus der Datenbank für die Domänenkonfiguration des Datenbankbenutzers. Wenn Sie diese Option weglassen, verwendet <i>infasetup</i> das in der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD angegebene Passwort. Wird in der Umgebungsvariable kein Wert angegeben, müssen Sie ein Passwort unter Verwendung dieser Option eingeben.
-DatabaseType -dt	Erforderlich. Typ der Datenbank, in der die Domänenkonfigurationsmetadaten gespeichert werden. Zu den Datenbanktypen gehören: <ul style="list-style-type: none"> <li>- db2</li> <li>- oracle</li> <li>- mssqlserver</li> <li>- sybase</li> <li>- postgresql</li> </ul>
-DatabaseServiceName -ds	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Der Name des Datenbankdiensts. Erforderlich für Oracle-, IBM DB2- und Microsoft SQL Server-Datenbanken. Geben Sie die SID für Oracle, den Dienstnamen für IBM DB2 oder den Datenbanknamen für Microsoft SQL Server ein.
-Tablespace -ts	Erforderlich für eine IBM DB2-Datenbank. Name des Tablespace, in dem sich die Datenbanktabellen für die Domänenkonfiguration befinden.
-SchemaName -sc	Optional. Name des Microsoft SQL Server-Schemas. Geben Sie einen Schemanamen ein, wenn Sie nicht das Standardschema verwenden.
-TrustedConnection -tc	Optional. Stellen Sie eine Verbindung zur Microsoft SQL Server-Datenbank über eine vertrauenswürdige Verbindung her. Die vertrauenswürdige Authentifizierung verwendet die Windows-Sicherheitsanmeldedaten des aktuellen Benutzers, um eine Verbindung zu Microsoft SQL Server herzustellen.
-KeysDirectory -kd	Optional. Verzeichnis, in dem alle Schlüsseltabellendateien und der Verschlüsselungsschlüssel für die Informatica-Domäne gespeichert werden. Standardwert ist <Informatica-Installationsverzeichnis>/isp/config/keys.

Option	Beschreibung
-DatabaseTlsEnabled -dbtls	Optional. Gibt an, ob die Informatica-Domänendatenbank mit TLS und SSL sicher ist. Setzen Sie diese Option für die sichere Datenbank auf True. Standardwert ist „False“. Wenn die Option -dbtls ohne Wert angegeben wird, verwendet die Informatica-Domäne die sichere Kommunikation mit der Informatica-Domänendatenbank.
-DatabaseTruststorePassword -dbtp	Optional. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.
-DatabaseTruststoreLocation -dbtl	Optional. Pfad und Dateiname der Truststore-Datei für den Gateway-Knoten.
-SingletonServiceParameters -ssp	Optional. Aktualisieren Sie die Serviceparameter mit einer der folgenden Optionen: <ul style="list-style-type: none"> <li>- SystemServicesFolderName</li> <li>- SchedulerService</li> <li>- ResourceManager</li> <li>- EmailService</li> </ul> <b>Syntax:</b> infasetup upgradeDomainMetadata -ssp <option>=<value>

## UpgradeGatewayNodeMetadata

Aktualisiert die Metadaten für einen Gateway-Knoten auf dem aktuellen Computer. Führen Sie vor dem Aktualisieren des Gateway-Knotens den Befehl „infacmd isp ShutDownNode“ aus, um den Knoten herunterzufahren.

Der Befehl „UpgradeGatewayNodeMetadata“ verwendet die folgende Syntax:

```

UpdateGatewayNode
[<-LogServiceDirectory|-ld> log_service_directory (used for GatewayNode only)]
[<-SystemLogDirectory|-sld> system_log_directory]
[<-HttpsPort|-hs> https_port]
[<-KeystoreFile|-kf> keystore_file_location]
[<-KeystorePass|-kp> keystore_password]
<<-DatabaseAddress|-da> database_hostname:database_port|<-DatabaseConnectionString|-cs>
database_connection_string>
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE|POSTGRESQL
[<-DatabaseServiceName|-ds> database_service_name]
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for MSSQLServer and PostgreSQL only)]
[<-TrustedConnection|-tc> trusted_connection (used for MSSQLServer only)]
<-PreviousInfaHome|-ph> previous_infa_home
[<-KeysDirectory|-kd> Infa_secrets_directory_location]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]

```

In der folgenden Tabelle werden *infasetup*-Optionen und -Argumente für „UpgradeGatewayNodeMetadata“ beschrieben:

Option	Beschreibung
-LogServiceDirectory -ld	Erforderlich. Freigegebener Verzeichnispfad, der vom Protokollmanager zum Speichern von Protokollereignisdateien verwendet wird. Stellen Sie sicher, dass -ld nicht übereinstimmt oder den angegebenen Wert für -sld enthält.
-SystemLogDirectory -sld	Optional. Verzeichnispfad zum Speichern von Systemprotokolldateien. Stellen Sie sicher, dass -ld nicht übereinstimmt oder den angegebenen Wert für -sld enthält. Standardwert ist <INFA_home>/logs.
-HttpsPort -hs	Optional. Portnummer, die vom Knoten für die Kommunikation zwischen dem Administrator Tool und dem Dienstmanager verwendet wird. Geben Sie diese Portnummer an, wenn Sie HTTPS für einen Knoten konfigurieren möchten.  Zum Deaktivieren von HTTPS-Unterstützung für einen Knoten setzen Sie diese Portnummer auf Null.
-KeystoreFile -kf	Optional. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die bei Verwendung des SSL-Protokolls erforderlich sind
-KeystorePass -kp	Optional. Ein Klartext-Passwort für die Schlüsselspeicherdatei. Sie können ein Passwort mit der Option -kp oder der Umgebungsvariable INFA_PASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -kp festgelegte Passwort Vorrang.
-DatabaseAddress -da	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Name und Portnummer des Computers, auf dem die Konfigurationsdatenbank der Domäne gehostet wird.
-DatabaseConnectionString -cs	Erforderlich, wenn Sie die Optionen -DatabaseAddress (-da) und -DatabaseServiceName (-ds) nicht verwenden. Verbindungszeichenfolge, die zum Herstellen einer Verbindung zur Konfigurationsdatenbank der Domäne verwendet wird. Geben Sie den Namen des Datenbankhosts, -ports und -diensts als Teil der Verbindungszeichenfolge ein. Setzen Sie die Verbindungszeichenfolge in Anführungszeichen.
-DatabaseUserName -du	Erforderlich, wenn Sie die Option -TrustedConnection (-tc) nicht verwenden. Konto für die Datenbank, die die Domänenkonfigurationsinformationen enthält.
-DatabasePassword -dp	Passwort aus der Datenbank für die Domänenkonfiguration des Datenbankbenutzers. Wenn Sie diese Option weglassen, verwendet <i>infasetup</i> das in der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD angegebene Passwort. Wird in der Umgebungsvariable kein Wert angegeben, müssen Sie ein Passwort unter Verwendung dieser Option eingeben.
-DatabaseType -dt	Erforderlich. Typ der Datenbank, in der die Domänenkonfigurationsmetadaten gespeichert werden. Zu den Datenbanktypen gehören: <ul style="list-style-type: none"> <li>- db2</li> <li>- oracle</li> <li>- mssqlserver</li> <li>- sybase</li> <li>- postgresql</li> </ul>

Option	Beschreibung
-DatabaseServiceName -ds	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Der Name des Datenbankdiensts. Erforderlich für Oracle-, IBM DB2- und Microsoft SQL Server-Datenbanken. Geben Sie die SID für Oracle, den Dienstnamen für IBM DB2 oder den Datenbanknamen für Microsoft SQL Server ein.
-Tablespace -ts	Erforderlich für eine IBM DB2-Datenbank. Name des Tablespace, in dem sich die Datenbanktabellen für die Domänenkonfiguration befinden.
-SchemaName -sc	Optional. Name des Microsoft SQL Server-Schemas. Geben Sie einen Schemanamen ein, wenn Sie nicht das Standardschema verwenden.
-TrustedConnection -tc	Optional. Stellen Sie eine Verbindung zur Microsoft SQL Server-Datenbank über eine vertrauenswürdige Verbindung her. Die vertrauenswürdige Authentifizierung verwendet die Windows-Sicherheitsanmeldedaten des aktuellen Benutzers, um eine Verbindung zu Microsoft SQL Server herzustellen.
-PreviousInfraHome -ph	Erforderlich. Pfad zum vorherigen Informatica-Startverzeichnis.
-KeysDirectory -kd	Optional. Verzeichnis, in dem alle Schlüsseltabellendateien und der Verschlüsselungsschlüssel für die Informatica-Domäne gespeichert werden. Standardwert ist <Informatica-Installationsverzeichnis>/isp/config/keys.
-DatabaseTlsEnabled -dbtls	Optional. Gibt an, ob die Informatica-Domänendatenbank mit TLS und SSL sicher ist. Setzen Sie diese Option für die sichere Datenbank auf True. Standardwert ist „False“. Wenn die Option -dbtls ohne Wert angegeben wird, verwendet die Informatica-Domäne die sichere Kommunikation mit der Informatica-Domänendatenbank.
-DatabaseTruststorePassword -dbtp	Optional. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.
-DatabaseTruststoreLocation -dbtl	Optional. Pfad und Dateiname der Truststore-Datei für den Gateway-Knoten.

## UnlockUser

Entsperrt ein natives oder ein LDAP-Benutzerkonto. Wenn Sie ein natives Benutzerkonto entsperren, können Sie außerdem ein neues Passwort für das Benutzerkonto eingeben.

Sie können ein Benutzerkonto entsperren, nachdem Sie die Domäne aus dem Gateway-Knoten herunterfahren.

Der Befehl „infasetup-Befehl UnlockUser“ verwendet folgende Syntax:

```
UnlockUser
<-UserName|-un> user_name
[<-SecurityDomain|-sdn] security domain]
[<-NewPassword|-np] new_password]
```



Die folgende Tabelle beschreibt die infasetup-Optionen und Argumente für UnlockUser:

Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich. Benutzername des gesperrten Kontos. Bei diesem Wert muss die Groß-/Kleinschreibung beachtet werden.
-SecurityDomain -sdn	sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung.  Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-NewPassword -np	new_password	Optional. Neues Passwort für das gesperrte native Konto.  Wenn Sie für ein natives Benutzerkonto die Passwortkomplexität aktivieren, beachten Sie beim Erstellen oder Ändern eines Passworts Folgendes: <ul style="list-style-type: none"> <li>- Das Passwort muss aus mindestens acht Zeichen bestehen.</li> <li>- Es muss mindestens einen Buchstaben, eine Zahl und ein nicht alphanumerisches Zeichen enthalten, z. B.:  <pre>! \ " # \$ % &amp; ' ( ) * + , - . / : ; &lt; = &gt; ? @ [ ] ^ _ ` {   } ~</pre> </li> </ul> Manche Sonderzeichen in Passwörtern können von der Shell anders interpretiert werden. Beispielsweise wird \$ als Variable interpretiert. Setzen Sie in diesem Fall ein Escape-Zeichen vor das betreffende Sonderzeichen.

## ValidateandRegisterFeature

Validiert und registriert die Funktion in der Domäne.

Der Befehl ValidateandRegisterFeature verwendet die folgende Syntax:

```
ValidateandRegisterFeature
<-FeatureFilename|-ff> feature_filename
<-IsUpgrade|-up> is_upgrade
```

In der folgenden Tabelle werden die *infasetup* ValidateandRegisterFeature-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-FeatureFilename -ff	feature_filename	Erforderlich. Speicherort der XML-Datei für das Plug-In.
-IsUpgrade -up	is_upgrade	Erforderlich. Gibt an, ob ein Upgrade des Plug-In auf die angegebene Version in der Funktionsdatei durchgeführt werden soll. Gültige Werte sind „True“ und „False“. Standardwert ist „True“.

# KAPITEL 43

## Pmcmd-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [Verwenden von pmcmd, 1392](#)
- [aborttask, 1397](#)
- [abortworkflow, 1399](#)
- [Connect, 1401](#)
- [Disconnect, 1402](#)
- [Exit, 1403](#)
- [getrunningsessionsdetails, 1403](#)
- [GetServiceDetails, 1404](#)
- [getserviceproperties, 1406](#)
- [getsessionstatistics, 1407](#)
- [gettaskdetails, 1409](#)
- [getworkflowdetails, 1411](#)
- [help, 1415](#)
- [pingservice, 1415](#)
- [recoverworkflow, 1416](#)
- [scheduleworkflow, 1418](#)
- [SetFolder, 1420](#)
- [SetNoWait, 1420](#)
- [SetWait, 1421](#)
- [ShowSettings, 1421](#)
- [StartTask, 1421](#)
- [StartWorkflow, 1425](#)
- [StopTask, 1429](#)
- [StopWorkflow, 1431](#)
- [UnscheduleWorkflow, 1433](#)
- [UnsetFolder, 1435](#)
- [Version, 1435](#)
- [WaitTask, 1435](#)
- [WaitWorkflow, 1437](#)

# Verwenden von pmcmd

*pmcmd* ist ein Programm zum Kommunizieren mit dem Integration Service. Mit *pmcmd* können Sie einige der Arbeiten ausführen, die Sie auch im Workflow Manager durchführen können, wie z. B. das Starten und Beenden von Arbeitsabläufen und Sitzungen.

Verwenden Sie *pmcmd* in den folgenden Modi:

- **Befehlszeilenmodus.** Sie rufen *pmcmd* jedes Mal auf und beenden es, wenn Sie einen Befehl ausführen. Sie können Skripts zum Planen von Arbeitsabläufen mit der Befehlszeilensyntax schreiben. Jeder im Befehlszeilenmodus geschriebene Befehl muss Verbindungsinformationen zum Integration Service einbeziehen.
- **Interaktiver Modus.** Sie stellen eine aktive Verbindung zum Integration Service her und erhalten sie aufrecht. Dadurch können Sie eine Reihe von Befehlen eingeben.

Sie können Umgebungsvariablen für Benutzernamen und Passwörter mit *pmcmd* verwenden. Sie können Umgebungsvariablen zudem verwenden, um die Art und Weise anzupassen, mit der *pmcmd* Datum und Uhrzeit auf dem Computer anzeigt, auf dem der Integration Service-Prozess ausgeführt wird. Bevor Sie *pmcmd* verwenden, konfigurieren Sie diese Variablen auf dem Computer, auf dem der Integration Service-Prozess ausgeführt wird. Die Umgebungsvariablen gelten für *pmcmd*-Befehle, die auf dem Knoten ausgeführt werden.

**Hinweis:** Wenn die Domäne eine Domäne für verschiedene Versionen ist, führen Sie *pmcmd* über das Installationsverzeichnis der Integration Service-Version aus.

## Ausführen von Befehlen im Befehlszeilenmodus

Im Befehlszeilenmodus wird *pmcmd* jedes Mal aufgerufen und beendet, wenn Sie einen Befehl ausführen. Der Befehlszeilenmodus ist sinnvoll, wenn Sie *pmcmd*-Befehle mit Batchdateien, Skripts oder anderen Programmen ausführen möchten.

Sie können *pmcmd*-Befehle mit Betriebssystem-Planungstools wie *cron* verwenden oder *pmcmd*-Befehle in Shell- oder Perl-Skripts einbetten.

Wenn Sie *pmcmd* im Befehlszeilenmodus ausführen, geben Sie in jedem Befehl Verbindungsinformationen wie Domänenname, Name des Integration Service, Benutzername und Passwort ein. Um beispielsweise den Arbeitsablauf "wf\_SalesAvg" im Ordner "SalesEast" zu starten, verwenden Sie folgende Syntax:

```
pmcmd startworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f SalesEast  
wf_SalesAvg
```

Der Benutzer "seller3" mit dem Passwort "jackson" sendet die Anfrage, um den Arbeitsablauf zu starten.

Wenn Sie eine erforderliche Option nicht oder falsch eingeben, schlägt der Befehl fehl und *pmcmd* gibt einen Nicht-Null-Rückgabewert zurück. Weitere Informationen über alle Rückgabewerte finden Sie unter ["pmcmd-Rückgabewerte" auf Seite 1393](#)

So führen Sie *pmcmd*-Befehle im Befehlszeilenmodus aus:

1. Wechseln Sie an der Eingabeaufforderung zu dem Verzeichnis, in dem sich die ausführbare *pmcmd*-Datei befindet.

Standardmäßig installiert das PowerCenter-Installationsprogramm *pmcmd* im \server\bin-Verzeichnis.

2. Geben Sie *pmcmd* gefolgt vom Befehlsnamen und den erforderlichen Optionen und Argumenten ein:

```
pmcmd command_name [-option1] argument_1 [-option2] argument_2...
```

## pmcmd-Rückgabewerte

Im Befehlszeilenmodus gibt *pmcmd* die erfolgreiche oder fehlgeschlagene Ausführung eines Befehls durch einen Rückgabewert an. Rückgabewert "0" gibt an, dass der Befehl erfolgreich ausgeführt wurde. Jeder andere Rückgabewert gibt an, dass der Befehl fehlgeschlagen ist.

Verwenden Sie den DOS- oder UNIX-echo-Befehl unmittelbar nach Ausführung eines *pmcmd*-Befehls, um den Rückgabewert für den Befehl anzuzeigen:

- An einer DOS-Shell: `echo %ERRORLEVEL%`
- An einer UNIX Bourne- oder Korn-Shell: `echo $?`
- An einer UNIX C-Shell: `echo $status`

In der folgenden Tabelle werden die Rückgabewerte für *pmcmd* beschrieben:

Code	Beschreibung
0	Für alle Befehle gibt ein Rückgabewert von Null an, dass der Befehl erfolgreich ausgeführt wurde. Sie können folgende Befehle im wait- oder nowait-Modus ausführen: starttask, startworkflow, aborttask und abortworkflow. Wenn Sie einen Befehl im wait-Modus ausführen, gibt ein Rückgabewert von Null an, dass der Befehl erfolgreich ausgeführt wurde. Wenn Sie einen Befehl im nowait-Modus ausführen, gibt ein Rückgabewert von Null an, dass die Anfrage erfolgreich an den Integration Service übermittelt wurde und dieser die Anfrage bestätigt hat.
1	Der Integration Service ist nicht verfügbar oder <i>pmcmd</i> kann keine Verbindung zum Integration Service herstellen. Es gibt ein Problem mit dem TCP/IP-Hostnamen, der Portnummer oder dem Netzwerk.
2	Der Name der Aufgabe, des Arbeitsablaufs oder des Ordners ist nicht vorhanden.
3	Beim Starten oder Ausführen des Arbeitsablaufs oder der Aufgabe ist ein Fehler aufgetreten.
4	Verwendungsfehler. Sie haben die falschen Optionen an <i>pmcmd</i> übergeben.
5	Ein interner <i>pmcmd</i> -Fehler ist aufgetreten. Setzen Sie sich mit dem globalen Informatica-Kundensupport in Verbindung.
7	Sie haben einen ungültigen Benutzernamen oder ein ungültiges Passwort verwendet.
8	Sie verfügen nicht über die entsprechenden Berechtigungen zum Ausführen dieser Aufgabe.
9	Die Verbindung zum Integration Service ist beim Senden der Anfrage abgelaufen.
12	Der Integration Service kann die Wiederherstellung nicht starten, da die Sitzung oder der Arbeitsablauf geplant ist, auf ein Ereignis wartet, wartet, initialisiert bzw. angehalten, aktiviert oder ausgeführt wird.
13	Die Benutzername-Umgebungsvariable ist auf einen leeren Wert gesetzt.
14	Die Passwort-Umgebungsvariable ist auf einen leeren Wert gesetzt.
15	Die Benutzername-Umgebungsvariable fehlt.
16	Die Passwort-Umgebungsvariable fehlt.
17	Die Parameterdatei ist nicht vorhanden.
18	Der Integration Service hat die Parameterdatei gefunden, verfügt aber nicht über die Anfangswerte für die Sitzungsparameter, wie beispielsweise \$input oder \$output.

Code	Beschreibung
19	Der Integration Service kann die Sitzung nicht wiederaufnehmen, da der Arbeitsablauf für eine kontinuierliche Ausführung konfiguriert wurde.
20	Ein Repository-Fehler ist aufgetreten. Stellen Sie sicher, dass der Repository Service und die Datenbank ausgeführt werden und die Anzahl der Verbindungen in der Datenbank nicht überschritten wird.
21	Der Integration Service wird heruntergefahren und akzeptiert keine neuen Anfragen.
22	Der Integration Service kann keine eindeutige Instanz des angegebenen Arbeitsablaufs/der angegebenen Sitzung finden. Geben Sie den Befehl erneut mit dem Namen des Ordners und des Arbeitsablaufs ein.
23	Für die Anfrage stehen keine Daten zur Verfügung.
24	Keine Speicherkapazität.
25	Befehl wird abgebrochen.

## Ausführen von Befehlen im interaktiven Modus

Verwenden Sie *pmcmd* im interaktiven Modus zum Starten und Stoppen von Arbeitsabläufen und Sitzungen, ohne ein Skript zu schreiben. Wenn Sie den interaktiven Modus verwenden, geben Sie Verbindungsinformationen wie Domänenname, Name des Integration Service, Benutzername und Passwort ein. Sie können nachfolgende Befehle ausführen, ohne die Verbindungsinformationen für jeden Befehl einzugeben.

Die folgenden Befehle rufen beispielsweise den interaktiven Modus auf, stellen eine Verbindung zum Integration Service "myintservice" her und starten die Arbeitsabläufe "wf\_SalesAvg" und "wf\_SalesTotal" im Ordner "SalesEast":

```
pmcmd
pmcmd> connect -sv MyIntService -d MyDomain -u seller3 -p jackson
pmcmd> setfolder SalesEast
pmcmd> startworkflow wf_SalesAvg
pmcmd> startworkflow wf_SalesTotal
```

So führen Sie *pmcmd*-Befehle im interaktiven Modus aus:

1. Wechseln Sie an der Eingabeaufforderung zu dem Verzeichnis, in dem sich die ausführbare *pmcmd*-Datei befindet.

*Standardmäßig installiert das PowerCenter-Installationsprogramm pmcmd im \server\bin-Verzeichnis.*

2. Geben Sie an der Eingabeaufforderung *pmcmd* ein.

Dies startet *pmcmd* im interaktiven Modus und zeigt die *pmcmd>*-Eingabeaufforderung an. *pmcmd* muss nicht vor jedem Befehl im interaktiven Modus eingegeben werden.

3. Geben Sie die Verbindungsinformationen für die Domäne und den Integration Service ein. Beispiel:

```
connect -sv MyIntService -d MyDomain -u seller3 -p jackson
```

4. Geben Sie einen Befehl und dessen Optionen und Argumente in folgendem Format ein:

```
command_name [-option1] argument_1 [-option2] argument_2...
```

*pmcmd* führt den Befehl aus und zeigt die Eingabeaufforderung erneut an.

5. Geben Sie *exit* ein, um eine interaktive Sitzung zu beenden.

## Festlegen von Standardwerten

Nachdem Sie eine Verbindung zu einem Integration Service mit *pmcmd* hergestellt haben, können Sie Standardordner oder Bedingungen festlegen, die jedes Mal verwendet werden sollen, wenn der Integration Service einen Befehl ausführt. Wenn Sie beispielsweise eine Reihe von Befehlen oder Aufgaben im selben Ordner eingeben möchten, geben Sie den Namen des Ordners mit dem *setfolder*-Befehl an. Alle nachfolgenden Befehle verwenden standardmäßig diesen Ordner.

In der folgenden Tabelle werden die Befehle beschrieben, mit denen Sie Standardwerte für nachfolgende Befehle festlegen:

Befehl	Beschreibung
setfolder	Legt einen Ordner als Standardordner fest, in dem alle nachfolgenden Befehle ausgeführt werden sollen.
setnowait	Führt nachfolgende Befehle im nowait-Modus aus. Die <i>pmcmd</i> -Eingabeaufforderung ist verfügbar, nachdem der Integration Service den vorangegangenen Befehl erhalten hat. Der nowait-Modus fungiert als Standardmodus.
setwait	Führt nachfolgende Befehle im wait-Modus aus. Die <i>pmcmd</i> -Eingabeaufforderung steht nach Abschluss des vorherigen Befehls durch den Integration Service zur Verfügung.
unsetfolder	Keht den <i>setfolder</i> -Befehl um.

Sie können mit dem *pmcmd* ShowSettings-Befehl die Standardeinstellungen anzeigen.

## Ausführen im wait-Modus

Sie können *pmcmd* im wait- oder nowait-Modus ausführen. Im wait-Modus kehrt *pmcmd* nach Abschluss des Befehls zur Shell oder Eingabeaufforderung zurück. Nachfolgende Befehle können erst ausgeführt werden, wenn der vorherige Befehl abgeschlossen ist.

Wenn Sie beispielsweise folgenden Befehl eingeben, startet *pmcmd* den Arbeitsablauf "wf\_SalesAvg" und kehrt erst dann zur Eingabeaufforderung zurück, wenn der Arbeitsablauf abgeschlossen ist:

```
pmcmd startworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f SalesEast -  
wait wf_SalesAvg
```

Im nowait-Modus kehrt *pmcmd* sofort zur Shell oder Eingabeaufforderung zurück. Sie müssen nicht auf den Abschluss eines Befehls warten, bevor Sie den nächsten Befehl ausführen.

Wenn Sie beispielsweise die folgenden Befehle eingeben, startet *pmcmd* den Arbeitsablauf "wf\_SalesTotal" selbst dann, wenn der Arbeitsablauf "wf\_SalesAvg" noch ausgeführt wird:

```
pmcmd startworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f SalesEast  
wf_SalesAvg  
pmcmd startworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f SalesEast  
wf_SalesTotal
```

Standardmäßig führt *pmcmd* Befehle im nowait-Modus aus.

Sie können den wait-Modus im Befehlszeilen- oder interaktiven Modus konfigurieren. Verwenden Sie im Befehlszeilenmodus die Option *-wait*, um einen Befehl im wait-Modus auszuführen. Verwenden Sie im interaktiven Modus den Befehl *setwait* oder *setnowait*, bevor Sie nachfolgende Befehle eingeben.

## Scripting von pmcmd-Befehlen

Bei Einsatz von *pmcmd* verwenden Sie möglicherweise regelmäßig einige Befehle mit bestimmten Optionen und Argumenten. Sie verwenden *pmcmd* beispielsweise, um den Status des Integration Service zu überprüfen. In diesem Fall können Sie ein Skript oder eine Batchdatei erstellen, um einen oder mehrere *pmcmd*-Befehle einschließlich der zugehörigen Optionen und Argumente aufzurufen.

Sie können Skripts in Befehlszeilenmodus ausführen. Sie können *pmcmd*-Skripts nicht im interaktiven Modus ausführen.

Das folgende UNIX-Shell-Skript überprüft beispielsweise den Status von Integration Service "testService" und falls dieser ausgeführt wird, werden Details für die Sitzung "s\_testSessionTask" abgerufen:

```
#!/usr/bin/bash
# Sample pmcmd script
# Check if the service is alive

pmcmd pingservice -sv testService -d testDomain
if [ "$?" != 0 ]; then

    # handle error

    echo "Could not ping service"

    exit

fi
# Get service properties

pmcmd getserviceproperties -sv testService -d testDomain
if [ "$?" != 0 ]; then

    # handle error

    echo "Could not get service properties"

    exit

fi
# Get task details for session task "s_testSessionTask" of workflow

# "wf_test_workflow" in folder "testFolder"

pmcmd gettaskdetails -sv testService -d testDomain -u Administrator -p adminPass -folder
testFolder -workflow wf_test_workflow s_testSessionTask
if [ "$?" != 0 ]; then

    # handle error

    echo "Could not get details for task s_testSessionTask"

    exit

fi
```

## Eingeben von Befehlsoptionen

*pmcmd* bietet mehrere Möglichkeiten zur Eingabe bestimmter Befehlsoptionen und -argumente. Verwenden Sie beispielsweise zur Eingabe eines Passworts die folgende Syntax:

```
<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>
```

Um ein Passwort einzugeben, stellen Sie dem Passwort die Option *-password* oder *-p* voran:

```
-password ThePassword
or
-p ThePassword
```



Wenn Sie eine Passwort-Umgebungsvariable verwenden, stellen Sie dem Variablennamen die Option -pv oder -passwordvar voran:

```
-passwordvar PASSWORD  
or  
-pv PASSWORD
```

Wenn eine Befehlsoption Leerzeichen enthält, schließen Sie die Option in einfache oder doppelte Anführungszeichen ein. Verwenden Sie zum Beispiel einfache Anführungszeichen in der folgenden Syntax, um den Ordnernamen einzuschließen:

```
abortworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f 'quarterly sales' -  
wait wf_MyWorkflow
```

Um einen leeren String zu kennzeichnen, verwenden Sie zwei einfache Anführungszeichen (") oder zwei doppelte Anführungszeichen ("").

## aborttask

Bricht eine Aufgabe ab. Verwenden Sie diesen Befehl nur dann, wenn der Integration Service die Aufgabe bei Verwendung des Befehls stoptask nicht anhalten kann.

Der Befehl „pmcmd aborttask“ verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd aborttask  
  
<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>  
  
<<-user|-u> username|<-uservar|-uv> userEnvVar>  
  
<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>  
  
[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>  
userSecuritydomainEnvVar>]  
  
[<-folder|-f> folder]  
  
<-workflow|-w> workflow  
  
[<-runinsname|-rin> runInsName]  
  
[-wfrunid workflowRunId]  
  
[-wait|-nowait]  
  
taskInstancePath
```

Der Befehl „pmcmd aborttask“ verwendet die folgende Syntax im interaktiven Modus:

```
aborttask  
  
[<-folder|-f> folder]  
  
<-workflow|-w> workflow  
  
[<-runinsname|-rin> runInsName]  
  
[-wfrunid workflowRunId]  
  
[-wait|-nowait]  
  
taskInstancePath
```

In der folgenden Tabelle werden Optionen und Argumente des Befehls „*pmcmd aborttask*“ beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich im Befehlszeilenmodus. Name des Integrationsdiensts. Wird im interaktiven Modus nicht verwendet.
-domain -d	domain	Optional im Befehlszeilenmodus. Domänenname. Wird im interaktiven Modus nicht verwendet.
-timeout -t	timeout	Optional im Befehlszeilenmodus. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integrationsdienst herzustellen. Wird im interaktiven Modus nicht verwendet.  Wurde die Option „-timeout“ weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Der Standardwert ist 180.
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Umgebungsvariable für den Benutzernamen nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Gibt die Umgebungsvariable für den Benutzernamen an. Wird im interaktiven Modus nicht verwendet.
-password -p	password	Erforderlich im Befehlszeilenmodus, wenn Sie die Umgebungsvariable für das Passwort nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Umgebungsvariable für das Passwort. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Der Standardwert ist „Nativ“.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Umgebungsvariable für die Sicherheitsdomäne. Wird im interaktiven Modus nicht verwendet.
-folder -f	Ordnerfolder	Erforderlich, wenn der Aufgabenname im Repository nicht eindeutig ist. Name des Ordners, der die Aufgabe enthält.
-workflow -w	workflowArbeitsablauf	Erforderlich. Name des Arbeitsablaufs.

Option	Argument	Beschreibung
-warten-wait -nowait	-	Optional. Konfiguriert den Wartemodus: <ul style="list-style-type: none"> <li>- wartenwait. Sie können einen neuen <i>pmcmd</i>-Befehl erst eingeben, wenn der Integration Service den vorherigen Befehl ausgeführt hat.</li> <li>- nowait. Sie können einen neuen <i>pmcmd</i>-Befehl eingeben, wenn der Integration Service den vorherigen Befehl empfangen hat.</li> </ul> Standardwert ist „nowait“.
-runinsname -rn	runInsName	Name der Arbeitsablaufausführungsinstanz, die die abzubrechende Aufgabe enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus, die die abzubrechende Aufgabe enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. <b>Hinweis:</b> Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-	taskInstancePath	Gibt einen Aufgabennamen und dessen Position im Arbeitsablauf an. Befindet sich die Aufgabe in einem Arbeitsablauf, geben Sie nur den Aufgabennamen ein. Befindet sich die Aufgabe in einem Worklet, geben Sie „WorkletName.TaskName“ ein. Geben Sie „taskInstancePath“ als vollständig qualifizierte Zeichenfolge ein.

## abortworkflow

Bricht einen Arbeitsablauf ab. Verwenden Sie diesen Befehl nur dann, wenn der Integration Service den Arbeitsablauf bei Verwendung des Befehls `stopworkflow` nicht anhalten kann.

Der Befehl `abortworkflow` verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd abortworkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[-wait|-nowait]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

Der Befehl `abortworkflow` verwendet die folgende Syntax im interaktiven Modus:

```
abortworkflow
[<-folder|-f> folder]
[-wait|-nowait]
[<-runinsname|-rin> runInsName]
[-wfrunid workflowRunId]
workflow
```

In der folgenden Tabelle werden *pmcmd* `abortworkflow`-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich im Befehlszeilenmodus. Name des Integration Service. Wird im interaktiven Modus nicht verwendet.
-domain -d	domain	Optional im Befehlszeilenmodus. Domänenname. Wird im interaktiven Modus nicht verwendet.
-timeout -t	timeout	Optional im Befehlszeilenmodus. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integration Service herzustellen. Wird im interaktiven Modus nicht verwendet.  Wurde die -timeout-Option weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	password	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.

Option	Argument	Beschreibung
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-warten -nowait	-	Optional. Konfiguriert den Wartemodus: <ul style="list-style-type: none"> <li>- warten. Sie können einen neuen <i>pmcmd</i>-Befehl erst eingeben, wenn der Integration Service den vorherigen Befehl ausgeführt hat.</li> <li>- nowait. Sie können einen neuen <i>pmcmd</i>-Befehl eingeben, wenn der Integration Service den vorherigen Befehl empfangen hat.</li> </ul> Als Standardwert wird nowait verwendet.
-runinsname -rin	runInsName	Name der abzubrechenden Arbeitsablaufausführungsinstanz. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus, die abgebrochen werden soll. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. <b>Hinweis:</b> Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.

## Connect

Verbindet das *pmcmd*-Programm mit dem Integration Service im interaktiven Modus. Wenn Sie Verbindungsinformationen weglassen, werden Sie von *pmcmd* zur Eingabe der korrekten Daten aufgefordert. Nach erfolgreicher Verbindungsherstellung mithilfe von *pmcmd* können Sie Befehle verwenden, ohne erneut Verbindungsinformationen eingeben zu müssen.

Connect

```
<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>
<<-user|-u> username|<-uservar|-uv> userEnvVar>
<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>
[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]
```

**Hinweis:** Verwenden Sie diesen Befehl ausschließlich im interaktiven *pmcmd*-Modus.

In der folgenden Tabelle werden *pmcmd* Connect-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integration Service herzustellen.  Wurde die -timeout-Option weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.

## Disconnect

Trennt *pmcmd* vom Integration Service. Das *pmcmd*-Programm wird nicht geschlossen. Verwenden Sie diesen Befehl, wenn Sie eine Trennung von einem Integration Service vornehmen und eine Verbindung zu einem anderen Integration Service im interaktiven Modus herstellen möchten.

Der Befehl Disconnect verwendet folgende Syntax im interaktiven Modus:

```
Disconnect
```

**Hinweis:** Verwenden Sie diesen Befehl ausschließlich im interaktiven *pmcmd*-Modus.

## Exit

Trennt *pmcmd* vom Integration Service und schließt das *pmcmd*-Programm.

Der Befehl Exit verwendet die folgende Syntax im interaktiven Modus:

```
Exit
```

**Hinweis:** Verwenden Sie diesen Befehl ausschließlich im interaktiven *pmcmd*-Modus.

## getrunningsessionsdetails

Gibt die folgenden Details für alle Sitzungen an, die aktuell auf einem Integration Service ausgeführt werden:

- Integration Service-Status, Startzeit und aktuelle Zeit
- Ordner und Name des Arbeitsablaufs
- Worklet und Sitzungsinstantz
- Bei jeder Ausführung der Sitzung: Aufgabentyp, Startzeit, Ausführungsstatus, erster Fehlercode, zugeordneter Integration Service, Ausführungsmodus und Knotenname
- Für das Mapping in einer laufenden Sitzung: Name des Mappings, Sitzungsprotokolldatei, erster Fehlercode und Fehlermeldung, Anzahl der erfolgreichen und fehlgeschlagenen Quell- und Zielzeilen und der Anzahl der Transformationsfehlermeldungen
- Anzahl der Sitzungen, die im Integration Service ausgeführt werden

Der Befehl „*pmcmd getrunningsessionsdetails*“ verwendet die folgende Syntax im Befehlszeilenmodus:.

```
pmcmd getrunningsessionsdetails  
  
<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>  
  
<<-user|-u> username|<-uservar|-uv> userEnvVar>  
  
<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>  
  
[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>  
userSecuritydomainEnvVar>]
```

Der Befehl „*pmcmd getrunningsessionsdetails*“ verwendet die folgende Syntax im interaktiven Modus:

```
getrunningsessionsdetails
```

In der folgenden Tabelle werden die Optionen und Argumente für „*pmcmd getrunningssessionsdetails*“ beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integrationsdiensts.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integrationsdienst herzustellen.  Wurde die Option „-timeout“ weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Der Standardwert ist 180.
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Umgebungsvariable für den Benutzernamen nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Umgebungsvariable für den Benutzernamen an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	password	Erforderlich im Befehlszeilenmodus, wenn Sie die Umgebungsvariable für das Passwort nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Umgebungsvariable für das Passwort. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Standardwert ist „Nativ“.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Umgebungsvariable für die Sicherheitsdomäne. Wird im interaktiven Modus nicht verwendet.

## GetServiceDetails

Gibt die folgenden Informationen zu einem Integration Service zurück:

- Name des Integration Service, Status, Startzeit und die aktuelle Zeit
- Für jeden aktiven Arbeitsablauf: Ordnername, Name des Arbeitsablaufs, Version, Ausführungsstatus, erster Fehlercode, Startzeit, Protokolldatei, Ausführungstyp und Benutzer, der den Arbeitsablauf ausführt



- Für jede aktive Aufgabe: Ordnername, Name und Version des Arbeitsablaufs, Name und Version der Aufgabeninstanz, Aufgabentyp, Start- und Endzeit, Ausführungsstatus, erster Fehlercode, Fehlermeldung, zugeordneter Integration Service, Ausführungsmodus, Namen der Knoten, auf denen die Aufgabe ausgeführt wird
- Anzahl der geplanten, aktiven und wartenden Arbeitsabläufe und Sitzungen

Der Befehl `GetServiceDetails` verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd GetServiceDetails

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[-all|-running|-scheduled]
```

Der Befehl `GetServiceDetails` verwendet die folgende Syntax im interaktiven Modus:

```
GetServiceDetails

[-all|-running|-scheduled]
```

In der folgenden Tabelle werden *pmcmd* `GetServiceDetails`-Optionen und Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integration Service herzustellen.  Wurde die -timeout-Option weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	password	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.

Option	Argument	Beschreibung
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-all -running -scheduled	-	Optional. Gibt die Arbeitsabläufe an, für die Details zurückgegeben werden sollen: <ul style="list-style-type: none"> <li>- all. Gibt Statusdetails zu den geplanten und laufenden Arbeitsabläufen zurück.</li> <li>- running. Gibt Statusdetails zu aktiven Arbeitsabläufen zurück. Aktive Arbeitsabläufe, einschließlich laufenden, ausstehenden und ausgesetzten Arbeitsabläufen.</li> <li>- scheduled. Gibt Statusdetails zu den geplanten Arbeitsabläufen zurück.</li> </ul> Die Standardeinstellung ist "all".

## getserviceproperties

Gibt die folgenden Informationen über den PowerCenter Integration Service zurück:

- Domäne, in der der PowerCenter Integration Service ausgeführt wird
- Name und Version des PowerCenter Integration Service
- Ob der PowerCenter Integration Service die Ausführung von Debug-Mappings zulässt
- Datenverschiebungsmodus
- Zugeordneter Repository Service
- Aktuelle Zeitstempel und Startzeit
- Name des Rasters
- Namen, Knoten und Codeseiten für die zugeordneten PowerCenter Integration Service-Prozesse
- Betriebsmodus für den PowerCenter Integration Service

Der Befehl „pmcmd getserviceproperties“ verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd getserviceproperties
<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>
```

Der Befehl „pmcmd getserviceproperties“ verwendet die folgende Syntax im interaktiven Modus:

```
getserviceproperties
```

In der folgenden Tabelle werden die Optionen und Argumente für „pmcmd getserviceproperties“ beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des PowerCenter-Integrationsdiensts.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem PowerCenter-Integrationsdienst herzustellen.  Wurde die Option „-timeout“ weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Der Standardwert ist 180.

## getsessionstatistics

Gibt Sitzungsdetails und -statistiken zurück. Der Befehl gibt die folgenden Informationen zurück:

- Ordnername, Name des Arbeitsablaufs, Worklet oder Sitzungsinstanz und Mapping-Name
- Name und Speicherort der Sitzungsprotokolldatei
- Anzahl der erfolgreichen und fehlgeschlagenen Quell- und Zielzeilen
- Anzahl der Transformationsfehler
- Erster Fehlercode und Fehlermeldung
- Aufgabenausführungsstatus
- Name des zugeordneten Integration Service
- Raster und Namen der Knoten, auf denen die Sitzung ausgeführt wird

Der Befehl gibt auch die folgenden Informationen für jede Partition zurück:

- Partitionsname
- Für jede Transformation innerhalb einer Partition: Transformationsinstanz, Transformationsname, Anzahl der angewendeten, betroffenen und zurückgewiesenen Zeilen, Durchsatz, letzter Fehlercode, Start- und Endzeit

Der Befehl `getsessionstatistics` verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd getsessionstatistics

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]
```

```

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

<-workflow|-w> workflow

taskInstancePath

```

Der Befehl `getsessionstatistics` verwendet die folgende Syntax im interaktiven Modus:

```

getsessionstatistics

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

<-workflow|-w> workflow

taskInstancePath

```

In der folgenden Tabelle werden *pmcmd* `getsessionstatistics`-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integration Service herzustellen.  Wurde die -timeout-Option weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	password	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.

Option	Argument	Beschreibung
-usersecuritydomain -usd	usersecuritydomain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Optional im Befehlszeilenmodus. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Aufgabenname im Repository nicht eindeutig ist. Name des Ordners, der die Aufgabe enthält.
-runinsname -rn	runInsName	Name der Arbeitsablaufausführungsinstanz, die die Aufgabe enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus, die die Aufgabe enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. <b>Hinweis:</b> Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-workflow -w	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.
-	taskInstancePath	Erforderlich. Gibt einen Aufgabennamen und dessen Position im Arbeitsablauf an. Befindet sich die Aufgabe in einem Arbeitsablauf, geben Sie nur den Aufgabennamen ein. Befindet sich die Aufgabe in einem Worklet, geben Sie WorkletName.TaskName ein. Geben Sie taskInstancePath als vollständig qualifizierten String ein.

## gettaskdetails

Gibt die folgenden Informationen über eine Aufgabe zurück:

- Ordnername, Name des Arbeitsablaufs, Name der Aufgabeninstanz und Aufgabentyp
- Start- und Endzeit der letzten Ausführung
- Aufgabenausführungsstatus, erster Fehlercode und Fehlermeldung
- Raster und Namen der Knoten, auf denen die Aufgabe ausgeführt wird
- Name des zugeordneten Integration Service
- Aufgabenausführungsmodus

Handelt es sich bei der Aufgabe um eine Sitzung, gibt der Befehl darüber hinaus die folgenden Details zurück:

- Mapping und Name der Sitzungsprotokolldatei
- Erster Fehlercode und Meldung
- Erfolgreiche und fehlgeschlagene Quell- und Zieldateien

- Anzahl der Transformationsfehler

Der Befehl „`pmcmd gettaskdetails`“ verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd gettaskdetails

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout] <<-user|-u>
username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-runinsname|-rin> runInsName]

taskInstancePath
```

Der Befehl „`pmcmd gettaskdetails`“ verwendet folgende Syntax im interaktiven Modus:

```
gettaskdetails

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-runinsname|-rin> runInsName]

taskInstancePath
```

In der folgenden Tabelle werden die Optionen und Argumente für „`pmcmd gettaskdetails`“ beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integrationsdiensts.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integrationsdienst herzustellen.  Wurde die Option „-timeout“ weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Der Standardwert ist 180.
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Umgebungsvariable für den Benutzernamen nicht angeben. Benutzernamen. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Umgebungsvariable für den Benutzernamen an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.

Option	Argument	Beschreibung
-password -p	password	Erforderlich im Befehlszeilenmodus, wenn Sie die Umgebungsvariable für das Passwort nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Umgebungsvariable für das Passwort. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Der Standardwert ist „Nativ“.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Umgebungsvariable für die Sicherheitsdomäne. Wird im interaktiven Modus nicht verwendet.
-folder -f	folderOrdner	Erforderlich, wenn der Aufgabenname im Repository nicht eindeutig ist. Name des Ordners, der die Aufgabe enthält.
-workflow -w	workflowArbeitsablauf	Erforderlich, wenn der Aufgabenname im Repository nicht eindeutig ist. Name des Ordners, der die Aufgabe enthält.
-runinsname -rn	runInsName	Name der Arbeitsablaufausführungsinstanz, die die Aufgabe enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-	taskInstancePath	Erforderlich. Gibt einen Aufgabennamen und dessen Position im Arbeitsablauf an. Befindet sich die Aufgabe in einem Arbeitsablauf, geben Sie nur den Aufgabennamen ein. Befindet sich die Aufgabe in einem Worklet, geben Sie „WorkletName.TaskName“ ein. Geben Sie „taskInstancePath“ als vollständig qualifizierte Zeichenfolge ein.

## getworkflowdetails

Gibt die folgenden Informationen über einen Arbeitsablauf zurück:

- Ordner und Namen der Arbeitsabläufe
- Arbeitsablaufausführungsstatus
- Erster Fehlercode und Fehlermeldung
- Start- und Endzeit
- Name der Protokolldatei
- Arbeitsablaufausführungstyp
- Name des Benutzers, der den Arbeitsablauf zuletzt ausgeführt hat
- Name des zugeordneten Integration Service

Der Befehl `getworkflowdetails` verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd getworkflowdetails

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

Der Befehl `getworkflowdetails` verwendet die folgende Syntax im interaktiven Modus:

```
getworkflowdetails

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

In der folgenden Tabelle werden Optionen und Argumente von `pmcmd getworkflowdetails` beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integrationsdiensts.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integrationsdienst herzustellen.  Wurde die -timeout-Option weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Standardwert ist 180.
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.



Option	Argument	Beschreibung
-password -p	password	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Standardwert ist „Native“.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	Ordner	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-runinsname -rin	runInsName	Name der Arbeitsablauf-Ausführungsinstanz. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablauf-Ausführungsinstanz aus. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. <b>Hinweis:</b> Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-	Arbeitsablauf	Name des Arbeitsablaufs.

In der folgenden Tabelle werden die verschiedenen Arbeitsablaufstatus beschrieben:

Name des Status	Beschreibung
Abgebrochen	Der Abbruch des Arbeitsablaufs oder der Aufgabe erfolgt durch den Benutzer im Arbeitsablauf-Monitor oder über <i>pmcmd</i> . Der Integrationsdienst beendet den DTM-Prozess und bricht die Aufgabe ab. Sie können einen abgebrochenen Arbeitsablauf wiederherstellen, indem Sie den Arbeitsablauf für die Wiederherstellung aktivieren.
Abbrechen	Der Integrationsdienst ist dabei, den Arbeitsablauf abzuberechnen.
Deaktiviert	Die Option „Deaktiviert“ wird in den Eigenschaften des Arbeitsablaufs vom Benutzer ausgewählt. Der Integrationsdienst führt den deaktivierten Arbeitsablauf erst aus, wenn die Auswahl der Option „Deaktiviert“ aufgehoben wird.
Fehlgeschlagen	Der Arbeitsablauf schlägt im Integrationsdienst fehl, da Fehler aufgetreten sind. Ein fehlgeschlagener Arbeitsablauf kann nicht wiederhergestellt werden.
Vorbereitung zum Ausführen	Der Integrationsdienst wartet auf eine Ausführungssperre für den Arbeitsablauf.

Name des Status	Beschreibung
Ausführen	Der Integrationsdienst führt den Arbeitsablauf aus.
Geplant	Die Ausführung des Arbeitsablaufs wird vom Benutzer zu einem künftigen Datum geplant. Der Integrationsdienst führt den Arbeitsablauf für die Dauer des Plans aus.
Gestoppt	Der Arbeitsablauf oder die Aufgabe wird vom Benutzer im Arbeitsablauf-Monitor oder über <i>pmcmd</i> gestoppt. Der Integrationsdienst stoppt die Verarbeitung der Aufgabe und aller anderen Aufgaben im zugehörigen Pfad. Der Integrationsdienst setzt die Ausführung paralleler Aufgaben fort. Sie können einen gestoppten Arbeitsablauf wiederherstellen, indem Sie den Arbeitsablauf für die Wiederherstellung aktivieren.
Stoppen	Der Integrationsdienst ist dabei, den Arbeitsablauf zu stoppen.
Erfolgreich	Der Integrationsdienst hat den Arbeitsablauf erfolgreich abgeschlossen.
Unterbrochen	Der Integrationsdienst unterbricht den Arbeitsablauf, da eine Aufgabe fehlgeschlagen ist und keine anderen Aufgaben im Arbeitsablauf ausgeführt werden. Dieser Status ist verfügbar, wenn Sie die Option zum Unterbrechen bei Auftreten eines Fehlers ausgewählt haben. Sie können einen ausgesetzten Arbeitsablauf wiederherstellen.
Ausstehend	Eine Aufgabe im Arbeitsablauf schlägt fehl, während andere Aufgaben weiterhin ausgeführt werden. Der Integrationsdienst stoppt die Ausführung der fehlgeschlagenen Aufgabe und fährt mit der Ausführung der Aufgaben in anderen Pfaden fort. Dieser Status ist verfügbar, wenn Sie die Option zum Unterbrechen bei Auftreten eines Fehlers ausgewählt haben.
Beendet	Der Integrationsdienst wird beim Ausführen dieses Arbeitsablaufs oder dieser Aufgabe unerwartet beendet. Sie können einen beendeten Arbeitsablauf wiederherstellen, wenn Sie den Arbeitsablauf für die Wiederherstellung aktivieren.
Beenden	Der Integrationsdienst ist dabei, den Arbeitsablauf oder die Aufgabe zu beenden.
Unbekannter Status	Dieser Status wird in den folgenden Situationen angezeigt: <ul style="list-style-type: none"> <li>- Der Integration Service kann den Status des Arbeitsablaufs oder der Aufgabe nicht bestimmen.</li> <li>- Der Integration Service reagiert nicht auf ein Ping vom Arbeitsablauf-Monitor.</li> <li>- Der Arbeitsablauf-Monitor kann während des Zeitraums für das Belastbarkeits-Timeout keine Verbindung zum Integration Service herstellen.</li> </ul>
Außerplanmäßig	Ein Arbeitsablauf wird vom Benutzer aus dem Plan entfernt.
Warten	Der Integrationsdienst wartet auf verfügbare Ressourcen, um den Arbeitsablauf oder die Aufgabe auszuführen. Sie können beispielsweise die maximale Anzahl der laufenden Sitzungs- und Befehlsaufgaben, die pro Integrationsdienst-Prozess auf dem Knoten zulässig sind, auf 10 festlegen. Wenn der Integrationsdienst bereits 10 parallele Sitzungen ausführt, weisen alle anderen Arbeitsabläufe und Aufgaben den Status „Wartet“ auf, bis der Integrationsdienst wieder ausreichend freie Ressourcen hat, um weitere Aufgaben auszuführen.

Der Befehl `getworkflowdetails` zeigt die letzten Details des Arbeitsablauf-Ausführungstyps an. Arbeitsablaufausführungstypen beziehen sich auf die zum Starten des Arbeitsablaufs verwendete Methode.

In der folgenden Tabelle werden die verschiedenen Arbeitsablauf-Ausführungstypen mit dem Befehl `getworkflowdetails` beschrieben:

Arbeitsablaufausführungstypen	Beschreibung
Benutzeranfrage	Manuell gestarteter Arbeitsablauf.
Zeitplan	Arbeitsablauf wird zum geplanten Zeitpunkt ausgeführt.

# help

Gibt die Syntax für den angegebenen Befehl zurück. Wenn Sie den Befehlsnamen weglassen, listet *pmcmd* alle Befehle und deren Syntax auf.

Der Befehl „`pmcmd help`“ verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd help [command]
```

Der Befehl „`pmcmd help`“ verwendet die folgende Syntax im interaktiven Modus:

```
help [command]
```

In der folgenden Tabelle werden die Optionen und Argumente für „`pmcmd help`“ beschrieben:

Option	Argument	Beschreibung
-	command	Optional. Name des Befehls. Wenn Sie den Befehlsnamen weglassen, listet <i>pmcmd</i> alle Befehle und deren Syntax auf.

# pingservice

Stellt sicher, dass der Integration Service ausgeführt wird.

Der Befehl „`pmcmd pingservice`“ verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd pingservice  
  
<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>
```

Der Befehl „`pmcmd pingservice`“ verwendet die folgende Syntax im interaktiven Modus:

```
pingservice
```

In der folgenden Tabelle werden die Optionen und Argumente für „pmcmd pingservice“ beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integrationsdiensts.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integrationsdienst herzustellen.  Wurde die Option „-timeout“ weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Der Standardwert ist 180.

## recoverworkflow

Stellt ausgesetzte Arbeitsabläufe wieder her. Geben Sie zum Wiederherstellen eines Arbeitsablaufs den Namen und Ordner für den Arbeitsablauf ein. Der Integration Service stellt den Arbeitsablauf aus allen unterbrochenen und fehlgeschlagenen Worklets sowie aus allen ausgesetzten und fehlgeschlagenen Befehls-, E-Mail- und Sitzungsaufgaben wieder her.

Der Befehl „pmcmd recoverworkflow“ verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd recoverworkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-paramfile> paramfile]

[<-localparamfile|-lpf> localparamfile]

[-wait|-nowait]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

Der Befehl „pmcmd recoverworkflow“ verwendet die folgende Syntax im interaktiven Modus:

```
recoverworkflow

[<-folder|-f> folder]
```

```

[<-paramfile> paramfile]

[<-localparamfile|-lpf> localparamfile]

[-wait|-nowait]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow

```

In der folgenden Tabelle werden die Optionen und Argumente für „pmcmd recoverworkflow“ beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integrationsdiensts.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integrationsdienst herzustellen.  Wurde die Option „-timeout“ weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Der Standardwert ist 180.
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Umgebungsvariable für den Benutzernamen nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Umgebungsvariable für den Benutzernamen an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	password	Erforderlich im Befehlszeilenmodus, wenn Sie die Umgebungsvariable für das Passwort nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Umgebungsvariable für das Passwort. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Der Standardwert ist „Nativ“.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Umgebungsvariable für die Sicherheitsdomäne. Wird im interaktiven Modus nicht verwendet.

Option	Argument	Beschreibung
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-paramfile	paramfile	Optional. Bestimmt die bei Ausführung einer Aufgabe oder eines Arbeitsablaufs zu verwendende Parameterdatei. Sie überschreibt die konfigurierte Parameterdatei für den Arbeitsablauf oder die Aufgabe.
-localparamfile -lpf	localparamfile	Optional. Gibt die Parameterdatei auf einem lokalen Computer an, die von <i>pmcmd</i> beim Start eines Arbeitsablaufs verwendet wird.
-wait -nowait	-	Optional. Konfiguriert den Wartemodus: <ul style="list-style-type: none"> <li>- waitarten. Sie können einen neuen <i>pmcmd</i>-Befehl erst eingeben, wenn der Integration Service den vorherigen Befehl ausgeführt hat.</li> <li>- nowait. Sie können einen neuen <i>pmcmd</i>-Befehl eingeben, wenn der Integration Service den vorherigen Befehl empfangen hat.</li> </ul> Der Standardwert ist „nowait“.
-runinsname -rin	runInsName	Name der Arbeitsablaufausführungsinstanz, die wiederhergestellt werden soll. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus, die wiederhergestellt werden soll. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. <b>Hinweis:</b> Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-	workflow	Erforderlich. Name des Arbeitsablaufs.

## scheduleworkflow

Weist den Integration Service an, einen Arbeitsablauf zu planen. Verwenden Sie diesen Befehl zum erneuten Planen eines Arbeitsablaufs, der aus dem Plan entfernt wurde.

Der Befehl „*pmcmd scheduleworkflow*“ verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd scheduleworkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]
```

```
workflow
```

Der Befehl „pmcmd scheduleworkflow“ verwendet folgende Syntax im interaktiven Modus:

```
scheduleworkflow
```

```
[<-folder|-f> folder]
```

```
workflow
```

In der folgenden Tabelle werden die Optionen und Argumente für „pmcmd scheduleworkflow“ beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integrationsdiensts.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integrationsdienst herzustellen.  Wurde die Option „-timeout“ weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Der Standardwert ist 180.
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Umgebungsvariable für den Benutzernamen nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Umgebungsvariable für den Benutzernamen an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	password	Erforderlich im Befehlszeilenmodus, wenn Sie die Umgebungsvariable für das Passwort nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Umgebungsvariable für das Passwort. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Der Standardwert ist „Nativ“.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Umgebungsvariable für die Sicherheitsdomäne. Wird im interaktiven Modus nicht verwendet.

Option	Argument	Beschreibung
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-	workflow	Erforderlich. Name des Arbeitsablaufs.

## SetFolder

Legt einen Ordner als Standardordner fest, in dem alle nachfolgenden Befehle ausgeführt werden sollen. Nach Ausgabe dieses Befehls muss kein Ordnername für Arbeitsablauf-, Aufgaben- oder Sitzungsbefehle eingegeben werden. Wenn Sie nach dem Befehl SetFolder in einem Befehl einen Ordnernamen eingeben, überschreibt dieser Ordnername den Namen des Standardordners für ausschließlich diesen Befehl.

Der Befehl SetFolder verwendet folgende Syntax im interaktiven Modus:

```
SetFolder folder
```

**Hinweis:** Verwenden Sie diesen Befehl ausschließlich im interaktiven *pmcmd*-Modus.

In der folgenden Tabelle werden die *pmcmd* SetFolder-Option und das -Argument beschrieben:

Option	Argument	Beschreibung
-	folder	Erforderlich. Name des Ordners.

## SetNoWait

Sie können *pmcmd* im wait- oder nowait-Modus ausführen. Im wait-Modus kehrt *pmcmd* nach Abschluss des Befehls zur Shell oder Eingabeaufforderung zurück. Nachfolgende Befehle können erst ausgeführt werden, wenn der vorherige Befehl abgeschlossen ist. Im nowait-Modus kehrt *pmcmd* sofort zur Shell oder Eingabeaufforderung zurück. Sie müssen nicht auf den Abschluss eines Befehls warten, bevor Sie den nächsten Befehl ausführen.

Der Befehl SetNoWait führt *pmcmd* im nowait-Modus aus. Der nowait-Modus fungiert als Standardmodus.

Der Befehl SetNoWait verwendet die folgende Syntax im interaktiven Modus:

```
SetNoWait
```

Wenn Sie den nowait-Modus einrichten, verwenden Sie nach Ausführung des vorherigen Befehls durch den Integration Service die *pmcmd*-Eingabeaufforderung.

**Hinweis:** Verwenden Sie diesen Befehl ausschließlich im interaktiven *pmcmd*-Modus.



# SetWait

Sie können *pmcmd* im wait- oder nowait-Modus ausführen. Im wait-Modus kehrt *pmcmd* nach Abschluss des Befehls zur Shell oder Eingabeaufforderung zurück. Nachfolgende Befehle können erst ausgeführt werden, wenn der vorherige Befehl abgeschlossen ist. Im nowait-Modus kehrt *pmcmd* sofort zur Shell oder Eingabeaufforderung zurück. Sie müssen nicht auf den Abschluss eines Befehls warten, bevor Sie den nächsten Befehl ausführen.

Der Befehl SetWait führt *pmcmd* im wait-Modus aus. Die *pmcmd*-Eingabeaufforderung steht nach Abschluss des vorherigen Befehls durch den Integration Service zur Verfügung.

Der Befehl SetWait verwendet die folgende Syntax im interaktiven Modus:

```
SetWait
```

**Hinweis:** Verwenden Sie diesen Befehl ausschließlich im interaktiven *pmcmd*-Modus.

# ShowSettings

Gibt den Namen der Domäne, des Integration Service und Repositorys zurück, mit dem *pmcmd* verbunden ist. Angezeigt werden Benutzername, wait-Modus und Standardordner.

Der Befehl ShowSettings verwendet folgende Syntax im interaktiven Modus:

```
ShowSettings
```

**Hinweis:** Verwenden Sie diesen Befehl ausschließlich im interaktiven *pmcmd*-Modus.

# StartTask

Startet eine Aufgabe.

Der Befehl StartTask verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd StartTask

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-paramfile> paramfile]

[-wait|-nowait]

[<-recovery|-norecovery>]

[<-runinsname|-rin> runInsName]
```

```
taskInstancePath
```

Der Befehl `StartTask` verwendet die folgende Syntax im interaktiven Modus:

```
pmcmd StartTask  
[<-folder|-f> folder]  
  
<-workflow|-w> workflow  
  
<-paramfile> paramfile]  
  
[-wait|-nowait]  
  
[<-recovery|-norecovery>]  
  
[<-runinsname|-rin> runInsName]  
  
taskInstancePath
```

In der folgenden Tabelle werden *pmcmd* `StartTask`-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integration Service herzustellen.  Wurde die -timeout-Option weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	password	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.

Option	Argument	Beschreibung
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-workflow -w	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.
-paramfile	paramfile	Optional. Bestimmt die bei Ausführung einer Aufgabe oder eines Arbeitsablaufs zu verwendende Parameterdatei. Sie überschreibt die konfigurierte Parameterdatei für den Arbeitsablauf oder die Aufgabe.
-warten -nowait	-	Optional. Konfiguriert den Wartemodus: <ul style="list-style-type: none"> <li>- warten. Sie können einen neuen <i>pmcmd</i>-Befehl erst eingeben, wenn der Integration Service den vorherigen Befehl ausgeführt hat.</li> <li>- nowait. Sie können einen neuen <i>pmcmd</i>-Befehl eingeben, wenn der Integration Service den vorherigen Befehl empfangen hat.</li> </ul> Als Standardwert wird nowait verwendet.

Option	Argument	Beschreibung
-recovery -norecovery	-	<p>Optional. Handelt es sich bei der Aufgabe um eine Sitzung, führt der Integration Service die Sitzung basierend auf der konfigurierten Wiederherstellungsstrategie aus.</p> <ul style="list-style-type: none"> <li>- recovery. Bei Echtzeitsitzungen, die für die Wiederherstellung aktiviert sind, stellt der Integration Service die fehlgeschlagene Sitzung wieder her und beendet die Ausführung der verbleibenden Aufgaben im Arbeitsablauf.</li> </ul> <p>Die Wiederherstellungsoption stimmt mit der Recover Task-Option im Workflow Manager überein. Diese Option ist nicht anwendbar auf Sitzungen, für die keine Wiederherstellung aktiviert wurde.</p> <ul style="list-style-type: none"> <li>- norecovery. Bei Echtzeitsitzungen, die für die Wiederherstellung aktiviert sind, verarbeitet der Integration Service keine Wiederherstellungsdaten. Der Integration Service löscht vor dem Neustart der Aufgabe den Betriebsstatus sowie die Wiederherstellungsdatei oder -tabelle. Bei Sitzungen, für die keine Wiederherstellung aktiviert wurde, löscht der Integration Service den Betriebsstatus und startet die Aufgabe neu.</li> </ul> <p>Die Norecovery-Option stimmt mit der Cold Start Task-Option im Workflow Manager überein.</p> <p>Wenn Sie keine Optionen für Sitzungen bereitstellen, die für die Wiederherstellung aktiviert sind, führt der Integration Service die Sitzung im Recovery-Modus aus. Wenn Sie keine Optionen für Sitzungen bereitstellen, die nicht für die Wiederherstellung aktiviert sind, führt der Integration Service die Sitzung im Norecovery-Modus aus aus.</p>
-runinsname -rn	runInsName	Name der Arbeitsablaufausführungsinstanz, die die zu startende Aufgabe enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-	taskInstancePath	<p>Erforderlich. Gibt einen Aufgabennamen und dessen Position im Arbeitsablauf an. Befindet sich die Aufgabe in einem Arbeitsablauf, geben Sie nur den Aufgabennamen ein. Befindet sich die Aufgabe in einem Worklet, geben Sie WorkletName.TaskName ein. Geben Sie taskInstancePath als vollständig qualifizierten String ein.</p>

## Verwenden von Parameterdateien mit starttask

Beim Starten einer Aufgabe können Sie optional das Verzeichnis und den Namen der Parameterdatei eingeben. Der Integration Service führt die Aufgabe mit den in der Datei angegebenen Parametern aus.

UNIX Shell-Benutzer sollten den Parameterdateinamen in einfache Anführungszeichen setzen:

```
-paramfile '$PMRootDir/myfile.txt'
```

Für Benutzer der Windows-Eingabeaufforderung gilt, dass der Parameterdateiname keine Leerzeichen am Anfang oder Ende haben darf. Wenn der Name Leerzeichen enthält, setzen Sie den Dateinamen in doppelte Anführungszeichen:

```
-paramfile "$PMRootDir\my file.txt"
```

Wenn Sie einen *pmcmd*-Befehl schreiben, der eine Parameterdatei enthält, die sich auf einem anderen Computer befindet, verwenden Sie den Backslash (\) mit dem Dollarzeichen (\$). Damit wird sichergestellt, dass der Computer, auf dem die Variable definiert ist, die Prozessvariable erweitert.

```
pmcmd starttask -sv MyIntService -d MyDomain -uv USERNAME -pv PASSWORD -f east -w
wSalesAvg -paramfile '\$PMRootDir/myfile.txt' taskA
```

## StartWorkflow

Startet einen Arbeitsablauf.

Der Befehl *StartWorkflow* verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd StartWorkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-startfrom> taskInstancePath]

[<-recovery|-norecovery>]

[<-paramfile> paramfile]

[<-localparamfile|-lpf> localparamfile]

[<-osprofile|-o> OSUser]

[-wait|-nowait]

[<-runinsname|-rin> runInsName]

workflow
```

Der Befehl *StartWorkflow* verwendet die folgende Syntax im interaktiven Modus:

```
pmcmd StartWorkflow

[<-folder|-f> folder]

[<-startfrom> taskInstancePath [<-recovery|-norecovery>]]

[<-paramfile> paramfile]

[<-localparamfile|-lpf> localparamfile]

[<-osprofile|-o> osProfile]

[-wait|-nowait]

[<-runinsname|-rin> runInsName]

workflow
```

In der folgenden Tabelle werden *pmcmd* StartWorkflow-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integration Service herzustellen.  Wurde die -timeout-Option weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	password	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.

Option	Argument	Beschreibung
-startfrom	taskInstancePath	<p>Optional. Startet einen Arbeitsablauf aus einer angegebenen Aufgabe, taskInstancePath. Befindet sich die Aufgabe in einem Arbeitsablauf, geben Sie nur den Aufgabennamen ein. Befindet sich die Aufgabe in einem Worklet, geben Sie WorkletName.TaskName ein. Geben Sie taskInstancePath als vollständig qualifizierten String ein.</p> <p>Wenn Sie keinen Startpunkt angeben, startet der Arbeitsablauf bei der Startaufgabe.</p> <p>Handelt es sich bei der Aufgabe um eine Sitzung, legen Sie die -recovery- oder -norecovery-Option zum Ausführen der Sitzung basierend auf der konfigurierten Wiederherstellungsstrategie fest.</p>
-paramfile	paramfile	<p>Optional. Bestimmt die bei Ausführung einer Aufgabe oder eines Arbeitsablaufs zu verwendende Parameterdatei. Sie überschreibt die konfigurierte Parameterdatei für den Arbeitsablauf oder die Aufgabe.</p>
-recovery -norecovery	-	<p>Optional. Der Integration Service führt die Sitzung basierend auf der konfigurierten Wiederherstellungsstrategie aus.</p> <ul style="list-style-type: none"> <li>- recovery. Bei Echtzeitsitzungen, die für die Wiederherstellung aktiviert sind, stellt der Integration Service die fehlgeschlagene Sitzung wieder her und beendet die Ausführung der verbleibenden Aufgaben im Arbeitsablauf.</li> </ul> <p>Die Recovery-Option stimmt mit der Recover Workflow-Option im Workflow Manager überein. Diese Option ist nicht anwendbar auf Sitzungen, für die keine Wiederherstellung aktiviert wurde.</p> <ul style="list-style-type: none"> <li>- norecovery. Bei Echtzeitsitzungen, die für die Wiederherstellung aktiviert sind, verarbeitet der Integration Service keine Wiederherstellungsdaten. Der Integration Service löscht vor dem Neustart der Aufgabe den Betriebsstatus sowie die Wiederherstellungsdatei oder -tabelle. Bei Sitzungen, für die keine Wiederherstellung aktiviert wurde, löscht der Integration Service den Betriebsstatus und startet die Aufgabe neu.</li> </ul> <p>Die Norecovery-Option stimmt mit der Cold Start Workflow-Option im Workflow Manager überein.</p> <p>Wenn Sie keine Optionen für Sitzungen bereitstellen, die für die Wiederherstellung aktiviert sind, führt der Integration Service die Sitzung im Recovery-Modus aus. Wenn Sie keine Optionen für Sitzungen bereitstellen, die nicht für die Wiederherstellung aktiviert sind, führt der Integration Service die Sitzung im Norecovery-Modus aus.</p>
-localparamfile -lpf	localparamfile	<p>Optional. Gibt die Parameterdatei auf einem lokalen Computer an, die von <i>pmcmd</i> beim Start eines Arbeitsablaufs verwendet wird.</p>
-osprofile -o	osProfile	<p>Optional. Gibt das dem Arbeitsablauf zugewiesene Betriebssystemprofil an.</p>

Option	Argument	Beschreibung
-warten -nowait	-	Optional. Konfiguriert den Wartemodus: - warten. Sie können einen neuen <i>pmcmd</i> -Befehl erst eingeben, wenn der Integration Service den vorherigen Befehl ausgeführt hat. - nowait. Sie können einen neuen <i>pmcmd</i> -Befehl eingeben, wenn der Integration Service den vorherigen Befehl empfangen hat. Als Standardwert wird nowait verwendet.
-runinsname -rin	runInsName	Name der zu startenden Arbeitsablaufausführungsinstanz. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.

## Verwenden von Parameterdateien mit startworkflow

Beim Starten eines Arbeitsablaufs können Sie optional das Verzeichnis und den Namen der Parameterdatei eingeben. Der Integration Service führt den Arbeitsablauf mit den in der Datei angegebenen Parametern aus. UNIX Shell-Benutzer sollten den Parameterdateinamen in einfache Anführungszeichen setzen. Für Benutzer der Windows-Eingabeaufforderung gilt, dass der Parameterdateiname keine Leerzeichen am Anfang oder Ende haben darf. Wenn der Name Leerzeichen enthält, setzen Sie den Dateinamen in doppelte Anführungszeichen.

Verwenden Sie Parameterdateien auf den folgenden Computern:

- **Knoten, auf dem Integration Service ausgeführt wird.** Wenn Sie eine Parameterdatei verwenden, die sich auf dem Integration Service-Computer befindet, verwenden Sie die Option `-paramfile`, um den Speicherort und Namen der Parameterdatei anzugeben.

Verwenden Sie unter UNIX die folgende Syntax:

```
-paramfile '$PMRootDir/myfile.txt'
```

Verwenden Sie unter Windows die folgende Syntax:

```
-paramfile "$PMRootDir\my file.txt"
```

- **Lokaler Rechner.** Wenn Sie eine Parameterdatei verwenden, die sich auf dem Rechner befindet, auf dem *pmcmd* aufrufen wird, übergibt *pmcmd* die Variablen und Werte in der Datei an den Integration Service. Geben Sie beim Erfassen einer lokalen Parameterdatei den absoluten oder relativen Pfad zur Datei an. Verwenden Sie die Option `-localparamfile` oder `-lpf`, um den Speicherort und Namen der lokalen Parameterdatei anzugeben.

Verwenden Sie unter UNIX die folgende Syntax:

```
-lpf 'param_file.txt'
-lpf 'c:\Informatica\parameterfiles\param file.txt'
-localparamfile 'c:\Informatica\parameterfiles\param file.txt'
```

Verwenden Sie unter Windows die folgende Syntax:

```
-lpf param_file.txt
-lpf "c:\Informatica\parameterfiles\param file.txt"
-localparamfile param_file.txt
```



- **Gemeinsam genutzte Netzwerklaufwerke.** Wenn Sie eine Parameterdatei verwenden, die sich auf einem anderen Computer befindet, verwenden Sie den Backslash (\) mit dem Dollarzeichen (\$). Damit wird sichergestellt, dass der Computer, auf dem die Variable definiert ist, die Prozessvariable erweitert.

```
-paramfile '$PMRootDir/myfile.txt'
```

## StopTask

Hält eine Aufgabe an.

Der Befehl `StopTask` verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd StopTask

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

[-wait|-nowait]

taskInstancePath
```

Der Befehl `StopTask` verwendet folgende Syntax im interaktiven Modus:

```
pmcmd StopTask

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

[-wait|-nowait]

taskInstancePath
```

In der folgenden Tabelle werden *pmcmd* `StopTask`-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.

Option	Argument	Beschreibung
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integration Service herzustellen.  Wurde die -timeout-Option weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	password	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-workflow -w	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.
-runinsname -rn	runInsName	Name der Arbeitsablaufausführungsinstanz, die die anzuhaltende Aufgabe enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus, die die anzuhaltende Aufgabe enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. <b>Hinweis:</b> Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.

Option	Argument	Beschreibung
-warten -nowait	-	Optional. Konfiguriert den Wartemodus: <ul style="list-style-type: none"> <li>- warten. Sie können einen neuen <i>pmcmd</i>-Befehl erst eingeben, wenn der Integration Service den vorherigen Befehl ausgeführt hat.</li> <li>- nowait. Sie können einen neuen <i>pmcmd</i>-Befehl eingeben, wenn der Integration Service den vorherigen Befehl empfangen hat.</li> </ul> Als Standardwert wird nowait verwendet.
-	taskInstancePath	Erforderlich. Gibt einen Aufgabennamen und dessen Position im Arbeitsablauf an. Befindet sich die Aufgabe in einem Arbeitsablauf, geben Sie nur den Aufgabennamen ein. Befindet sich die Aufgabe in einem Worklet, geben Sie WorkletName.TaskName ein. Geben Sie taskInstancePath als vollständig qualifizierten String ein.

## StopWorkflow

Hält einen Arbeitsablauf an.

Der Befehl StopWorkflow verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd StopWorkflow

[<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

[<-user|-u> username|<-uservar|-uv> userEnvVar>

[<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

[-wait|-nowait]

workflow
```

Der Befehl StopWorkflow verwendet die folgende Syntax im interaktiven Modus:

```
pmcmd StopWorkflow

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

[-wait|-nowait]

workflow
```

In der folgenden Tabelle werden *pmcmd* StopWorkflow-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integration Service herzustellen.  Wurde die -timeout-Option weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	password	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-runinsname -rin	runInsName	Name der Arbeitsablaufausführungsinstanz, die angehalten werden soll. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.

Option	Argument	Beschreibung
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus, die angehalten werden soll. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. <b>Hinweis:</b> Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-warten -nowait	-	Optional. Konfiguriert den Wartemodus: - warten. Sie können einen neuen <i>pmcmd</i> -Befehl erst eingeben, wenn der Integration Service den vorherigen Befehl ausgeführt hat. - nowait. Sie können einen neuen <i>pmcmd</i> -Befehl eingeben, wenn der Integration Service den vorherigen Befehl empfangen hat. Als Standardwert wird nowait verwendet.
-	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.

## UnscheduleWorkflow

Entfernt einen Arbeitsablauf aus einem Zeitplan.

Der UnscheduleWorkflow-Befehl verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd UnscheduleWorkflow

[<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

[<-user|-u> username|<-uservar|-uv> userEnvVar>

[<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

workflow
```

Der UnscheduleWorkflow-Befehl verwendet die folgende Syntax im interaktiven Modus:

```
UnscheduleWorkflow

[<-folder|-f> folder]

workflow
```

In der folgenden Tabelle werden die *pmcmd* UnscheduleWorkflow-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integration Service herzustellen.  Wurde die -timeout-Option weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	password	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.

# UnsetFolder

Entfernt die Kennzeichnung eines Standardordners. Nachdem Sie diesen Befehl angewendet haben, müssen Sie einen Ordernamen jedes Mal angeben, wenn Sie einen Befehl für eine Sitzung, einen Arbeitsablauf oder eine Aufgabe eingeben.

Der UnsetFolder-Befehl verwendet die folgende Syntax im interaktiven Modus:

```
UnsetFolder
```

**Hinweis:** Verwenden Sie diesen Befehl ausschließlich im interaktiven *pmcmd*-Modus.

# Version

Zeigt die PowerCenter-Version und Informatica-Handelsmarke sowie Urheberrechtsinformationen an.

Der Version-Befehl verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd Version
```

Der Version-Befehl verwendet die folgende Syntax im interaktiven Modus:

```
Version
```

# WaitTask

Weist den Integration Service an, die Aufgabe abzuschließen, bevor die *pmcmd*-Eingabeaufforderung an die Befehlseingabeaufforderung oder Shell zurückgegeben wird.

Der WaitTask-Befehl verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd WaitTask

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

taskInstancePath
```

Der WaitTask-Befehl verwendet die folgende Syntax im interaktiven Modus:

```
WaitTask

[<-folder|-f> folder]

<-workflow|-w> workflow
```

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

taskInstancePath

In der folgenden Tabelle werden die *pmcmd* WaitTask-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integration Service herzustellen.  Wurde die -timeout-Option weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	password	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Aufgabenname im Repository nicht eindeutig ist. Name des Ordners, der die Aufgabe enthält.
-workflow -w	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.



Option	Argument	Beschreibung
-runinsname -rn	runInsName	Name der Arbeitsablaufausführungsinstanz, die die Aufgabe enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus, die die Aufgabe enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. <b>Hinweis:</b> Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-	taskInstancePath	Erforderlich. Gibt einen Aufgabennamen und dessen Position im Arbeitsablauf an. Befindet sich die Aufgabe in einem Arbeitsablauf, geben Sie nur den Aufgabennamen ein. Befindet sich die Aufgabe in einem Worklet, geben Sie WorkletName.TaskName ein. Geben Sie taskInstancePath als vollständig qualifizierten String ein.

## WaitWorkflow

Bewirkt, dass *pmcmd* auf den Abschluss eines Arbeitsablaufs wartet, bevor es nachfolgende Befehle ausführt. Verwenden Sie diesen Befehl in Verbindung mit dem Rückgabewert, wenn Sie *pmcmd* über ein Skript ausführen. Beispielsweise möchten Sie den Status eines kritischen Arbeitsablaufs prüfen, bevor ein anderer Arbeitsablauf gestartet wird. Verwenden Sie den WaitWorkflow-Befehl, um auf den Abschluss des kritischen Arbeitsablaufs zu warten, und überprüfen Sie dann den *pmcmd*-Rückgabewert. Wenn der Rückgabewert 0 ist (erfolgreich), starten Sie den nächsten Arbeitsablauf.

Der WaitWorkflow-Befehl gibt bei Abschluss eines Arbeitsablaufs die Eingabeaufforderung zurück.

Der WaitWorkflow-Befehl verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd WaitWorkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

Der WaitWorkflow-Befehl verwendet die folgende Syntax im interaktiven Modus:

```
WaitWorkflow

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]
```

```
[-wfrunid workflowRunId]
```

```
workflow
```

In der folgenden Tabelle werden die *pmcmd* WaitWorkflow-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem <i>pmcmd</i> versucht, eine Verbindung mit dem Integration Service herzustellen.  Wurde die -timeout-Option weggelassen, verwendet <i>pmcmd</i> den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet <i>pmcmd</i> den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	password	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-runinsname -rin	runInsName	Name der Arbeitsablaufausführungsinstanz Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.

Option	Argument	Beschreibung
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. <b>Hinweis:</b> Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.

# KAPITEL 44

## pmrep-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- [Verwenden von pmrep, 1442](#)
- [AddToDeploymentGroup, 1447](#)
- [ApplyLabel, 1449](#)
- [AssignIntegrationService, 1451](#)
- [AssignPermission, 1452](#)
- [BackUp, 1454](#)
- [ChangeOwner, 1455](#)
- [CheckIn, 1455](#)
- [CleanUp, 1456](#)
- [ClearDeploymentGroup, 1456](#)
- [Connect, 1457](#)
- [Create, 1459](#)
- [CreateConnection, 1460](#)
- [CreateDeploymentGroup, 1464](#)
- [CreateFolder, 1464](#)
- [CreateLabel, 1466](#)
- [CreateQuery, 1466](#)
- [Delete, 1472](#)
- [DeleteConnection, 1473](#)
- [DeleteDeploymentGroup, 1474](#)
- [DeleteFolder, 1474](#)
- [DeleteLabel, 1475](#)
- [DeleteObject, 1475](#)
- [DeleteQuery, 1476](#)
- [DeployDeploymentGroup, 1477](#)
- [DeployFolder, 1478](#)
- [ExecuteQuery, 1480](#)
- [Exit, 1482](#)
- [FindCheckout, 1482](#)
- [GetConnectionDetails, 1484](#)

- [GenerateAbapProgramToFile, 1484](#)
- [Hilfe, 1486](#)
- [InstallAbapProgram, 1486](#)
- [KillUserConnection, 1489](#)
- [ListConnections, 1489](#)
- [ListObjectDependencies , 1490](#)
- [ListObjects, 1492](#)
- [ListTablesBySess, 1498](#)
- [ListUserConnections, 1499](#)
- [MassUpdate, 1499](#)
- [ModifyFolder, 1505](#)
- [Benachrichtigen, 1507](#)
- [ObjectExport, 1507](#)
- [ObjectImport , 1509](#)
- [PurgeVersion, 1510](#)
- [Register, 1513](#)
- [RegisterPlugin, 1515](#)
- [Wiederherstellen, 1517](#)
- [RollbackDeployment , 1518](#)
- [Ausführen, 1519](#)
- [ShowConnectionInfo, 1520](#)
- [SwitchConnection, 1520](#)
- [TruncateLog, 1521](#)
- [UndoCheckout, 1522](#)
- [Unregister, 1523](#)
- [UnregisterPlugin, 1524](#)
- [UpdateConnection, 1526](#)
- [UpdateEmailAddr, 1528](#)
- [UpdateSeqGenVals, 1529](#)
- [UpdateSrcPrefix, 1530](#)
- [UpdateStatistics , 1531](#)
- [UpdateTargPrefix, 1532](#)
- [Upgrade, 1533](#)
- [UninstallAbapProgram, 1533](#)
- [Validieren, 1535](#)
- [Version, 1537](#)

# Verwenden von pmrep

*pmrep* ist ein Befehlszeilenprogramm, mit dem Sie Repository-Informationen aktualisieren und Repository-Funktionen ausführen können. *pmrep* wird in den bin-Verzeichnissen des PowerCenter Client und der PowerCenter-Dienste installiert.

Verwenden Sie *pmrep* zum Ausführen von Aufgaben zur Repository-Verwaltung, wie z. B. Auflisten von Repository-Objekten, Erstellen und Bearbeiten von Gruppen, Wiederherstellen und Löschen von Repositories und Aktualisieren von Parametern und Sicherheitsinformationen im Zusammenhang mit Sitzungen im PowerCenter Repository.

Beim Verwenden von *pmrep* können Sie Befehle in den folgenden Modi eingeben:

- **Befehlszeilenmodus.** Sie können *pmrep*-Befehle direkt über die Befehlszeile des Systems eingeben. Verwenden Sie den Befehlszeilenmodus, um *pmrep*-Befehle zu schreiben.
- **Interaktiver Modus.** Sie können *pmrep*-Befehle über eine interaktive Eingabeaufforderung eingeben. *pmrep* wird nach Abschluss des Befehls nicht beendet.

Sie können mit Umgebungsvariablen Benutzernamen und Passwörter für *pmrep* festlegen. Konfigurieren Sie vor der Verwendung von *pmrep* diese Umgebungsvariablen. Die Umgebungsvariablen gelten für *pmrep*-Befehle, die auf dem Knoten ausgeführt werden.

Alle *pmrep*-Befehle erfordern eine Verbindung zum Repository. Davon ausgenommen sind folgende Befehle:

- Hilfe
- ListAllPrivileges

Verwenden Sie den *pmrep* Connect-Befehl zum Herstellen einer Verbindung zum Repository, bevor Sie andere *pmrep*-Befehle verwenden.

**Hinweis:** Wenn die Domäne eine Domäne für verschiedene Versionen ist, führen Sie *pmrep* über das Installationsverzeichnis der Repository Service-Version aus.

## Ausführen von Befehlen im Befehlszeilenmodus

Im Befehlszeilenmodus wird *pmrep* jedes Mal aufgerufen und beendet, wenn Sie einen Befehl ausführen. Der Befehlszeilenmodus ist sinnvoll, wenn Sie *pmrep*-Befehle mit Batchdateien, Skripts oder anderen Programmen ausführen möchten.

So führen Sie *pmrep*-Befehle im Befehlszeilenmodus aus:

1. Ändern Sie an der Eingabeaufforderung das Verzeichnis, in dem sich die ausführbare *pmrep*-Datei befindet.
2. Geben Sie *pmrep* gefolgt vom Befehlsnamen und dessen Optionen und Argumenten ein:

```
pmrep command_name [-option1] argument_1 [-option2] argument_2...
```

## Ausführen von Befehlen im interaktiven Modus

Interaktiver Modus ruft *pmrep* auf. Sie können eine Reihe von Befehlen an einer *pmrep*-Eingabeaufforderung eingeben, ohne den Vorgang nach jedem Befehl zu beenden.

So führen Sie *pmrep*-Befehle im interaktiven Modus aus:

1. Geben Sie an der Eingabeaufforderung *pmrep* ein, um den interaktiven Modus aufzurufen.  
Dies startet *pmrep* im interaktiven Modus und zeigt eine *pmrep>*-Eingabeaufforderung an. *pmrep* muss nicht vor jedem Befehl im interaktiven Modus eingegeben werden.

2. Geben Sie einen Befehl und dessen Optionen und Argumente ein.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
command_name [-option1] argument_1 [-option2] argument_2...
```

*pmrep* führt den Befehl aus und zeigt die Eingabeaufforderung erneut an.

3. Geben Sie `exit` ein, um eine interaktive Sitzung zu beenden.

## Ausführen von Befehlen im normalen und exklusiven Modus

Der Repository Service wird im normalen oder exklusiven Modus ausgeführt. Führen Sie den Repository Service im exklusiven Modus aus, um Aufgaben durchzuführen, die nur eine Benutzerverbindung zum Repository zulassen.

Führen Sie den Repository Service im exklusiven Modus aus, um die folgenden *pmrep*-Befehle zu verwenden:

- Create
- Delete
- Register
- RegisterPlugin
- Unregister
- UnregisterPlugin

Sie können das Administrator-Tool oder *infacmd* zum Ausführen des Repository Service im exklusiven Modus verwenden.

## pmrep-Rückgabewerte

*pmrep* gibt die erfolgreiche oder fehlgeschlagene Ausführung eines Befehls mit einem Rückgabewert an. Rückgabewert "0" gibt an, dass der Befehl erfolgreich ausgeführt wurde. Rückgabewert "1" gibt an, dass der Befehl fehlgeschlagen ist. Bestimmte Befehle führen mehrere Operationen aus. Mit *AddToDeploymentgroup* werden einer Bereitstellungsgruppe beispielsweise mehrere Objekte hinzugefügt. In diesen Fällen gibt der Rückgabewert "0" an, dass der Befehl erfolgreich ausgeführt wurde, auch wenn nur bestimmte Objekte erfolgreich bereitgestellt wurden.

Geben Sie sofort nach der Ausführung des Befehls *pmrep* einen der folgenden DOS- oder UNIX-echo-Befehle ein:

- Geben Sie an einer DOS-Shell `echo %ERRORLEVEL%` ein
- Geben Sie an einer UNIX Bourne- oder Korn-Shell `echo $?` ein
- Geben Sie an einer UNIX C-Shell `echo $status` ein

## Verwenden von nativen Verbindungsstrings

Einige *pmrep*-Befehle, wie z. B. *CreateConnection* und *Restore*, erfordern einen nativen Verbindungsstring.

In der folgenden Tabelle wird die Syntax nativer Verbindungsstrings für die einzelnen unterstützten Datenbanken beschrieben:

Datenbank	Verbindungsstring-Syntax	Beispiel
IBM DB2	<i>dbname</i>	mydatabase
Microsoft SQL Server	<i>servername@dbname</i>	sqlserver@mydatabase
Oracle	<i>dbname.world</i> (identisch mit dem Eintrag TNSNAMES)	oracle.world
Sybase ASE	<i>servername@dbname</i>	sambrown@mydatabase

## pmrep-Scripting-Befehle

Bei Einsatz von *pmrep* verwenden Sie möglicherweise regelmäßig einige Befehle mit bestimmten Optionen und Argumenten. Sie können *pmrep* beispielsweise verwenden, um täglich ein Backup eines Produktions-Repositorys durchzuführen. In diesem Fall können Sie eine Skriptdatei erstellen, um einen oder mehrere *pmrep*-Befehle einschließlich der zugehörigen Optionen und Argumente aufzurufen.

Mit der Windows-Batchdatei "backupproduction.bat" kann beispielsweise eine Verbindung zu einem Repository mit der Bezeichnung "Produktion" hergestellt und dessen Sicherung durchgeführt werden.

```

backupproduction.bat
REM This batch file uses pmrep to connect to and back up the repository Production on
the server ServerName
@echo off
echo Connecting to repository Production...
c:\PowerCenter\pmrep\pmrep connect -r Production -n Administrator -x Adminpwd -d
MyDomain -h Machine -o 8080
echo Backing up repository Production...
c:\PowerCenter\pmrep\pmrep backup -o c:\backup\Production_backup.rep

```

Sie können Skriptdateien über die Befehlszeilenschnittstelle ausführen. Sie können *pmrep*-Batchdateien nicht im interaktiven Modus ausführen.

## Tipps für das Scripting von pmrep-Befehlen

Wenden Sie beim Erstellen und Ausführen von *pmrep*-Skripts die folgenden Tipps an:

- Fügen Sie einen Connect-Befehl als ersten Befehl ein, der von der Skriptdatei aufgerufen wird. Damit können Sie sicherstellen, dass die Aufgaben im richtigen Repository ausgeführt werden.
- Um *pmrep*-Skripts auszuführen, die Verbindungen zu unterschiedlichen Repositories gleichzeitig herstellen, legen Sie die Umgebungsvariable INFA\_REPCNX\_INFO in jeder Umgebung so fest, dass Name und Dateipfad für die Repository-Verbindungsdatei gespeichert werden. Dies verhindert, dass ein Skript die von einem anderen Skript verwendeten Verbindungsinformationen überschreibt.



## Verbindungsuntertypen

Wenn Sie eine Verbindung auflisten oder aktualisieren, können Sie die Verbindungsuntertypen basierend auf dem zugehörigen Verbindungstyp angeben. Der Befehl „pmrep“ listet basierend auf den Repository-Plug-Ins die Verbindungsuntertypen standardmäßig im Repository auf.

In der folgenden Tabelle wird die Liste der Verbindungsuntertypen für den zugehörigen Verbindungstyp angezeigt:

Typ der Verbindung	Verbindungsuntertyp
Relational	Sybase
Relational	Informix (veraltet)
Relational	Microsoft SQL Server
Relational	DB2
Relational	ODBC
Relational	Teradata
Relational	Netezza
Relational	Vertica
Relational	PowerChannel for DB2
Relational	PowerChannel for Oracle
Relational	PowerChannel for MS SQL Server
Relational	PowerChannel for ODBC
Relational	PWX DB2zOS
Relational	PWX DB2i5OS
Relational	PWX DB2LUW
Relational	PWX Oracle
Relational	PWX MSSQLServer
Relational	PWX NRDB Lookup
Relational	Teradata PT Connection
Anwendung	SAP BW
Anwendung	SAP R3
Anwendung	PeopleSoft Oracle
Anwendung	PeopleSoft Sybase

Typ der Verbindung	Verbindungsuntertyp
Anwendung	PeopleSoft Informix
Anwendung	PeopleSoft MsSqlserver
Anwendung	PeopleSoft Db2
Anwendung	Siebel Oracle
Anwendung	Siebel Sybase
Anwendung	Siebel Informix
Anwendung	Siebel MsSqlserver
Anwendung	Siebel Db2
Anwendung	SAP_ALE_IDoc_Reader
Anwendung	SAP Type A
Anwendung	SAP_BWOHS_READER
Anwendung	SAP_ALE_IDoc_Writer
Anwendung	SAP RFC/BAPI Interface
Anwendung	JNDI Connection
Anwendung	JMS Connection
Anwendung	webMethods Broker
Anwendung	webMethods Integration Server
Anwendung	Web Services Consumer
Anwendung	PWX NRDB Batch
Anwendung	PWX NRDB CDC Change
Anwendung	PWX NRDB CDC Real Time
Anwendung	PWX DB2zOS CDC Change
Anwendung	PWX DB2zOS CDC Real Time
Anwendung	PWX DB2i5OS CDC Change
Anwendung	PWX DB2i5OS CDC Real Time
Anwendung	Http Transformation
Anwendung	PWX Oracle CDC Change

Typ der Verbindung	Verbindungsuntertyp
Anwendung	PWX Oracle CDC Real Time
Anwendung	LMAPITarget
Anwendung	Teradata FastExport Connection
Anwendung	PWX MSSQL CDC Change
Anwendung	PWX MSSQL CDC Real Time
Anwendung	PWX DB2LUW CDC Change
Anwendung	PWX DB2LUW CDC Real Time
Anwendung	Salesforce Connection
Anwendung	Hadoop HDFS Connection
FTP	FTP
Externer Ladevorgang	Teradata Mload External Loader
Externer Ladevorgang	Teradata Tpump External Loader
Externer Ladevorgang	DB2 EE External Loader
Externer Ladevorgang	DB2 EEE External Loader
Externer Ladevorgang	Teradata FastLoad External Loader
Externer Ladevorgang	Teradata Warehouse Builder External Loader
Externer Ladevorgang	HP NeoView Java Transporter
Warteschlange	Message Queue
Warteschlange	MSMQ

## AddToDeploymentGroup

Fügt Objekte einer Bereitstellungsgruppe hinzu. Verwenden Sie AddToDeploymentGroup zum Hinzufügen von Quelle, Target, Transformation, Mapping, Sitzung, Worklet, Arbeitsablauf, Scheduler, Sitzungskonfiguration und Aufgabenobjekten.

Sie können keine ausgecheckten Objekte zu einer Bereitstellungsgruppe hinzufügen. Sie können Objekte mit Befehlsoptionen angeben oder eine persistente Eingabedatei verwenden. Bei Verwendung einer persistenten Eingabedatei können Sie die Option für den Bereitstellungsgruppennamen eingeben.

Verwenden Sie AddToDeploymentGroup, um wiederverwendbare Eingabeobjekte hinzuzufügen. Wenn Sie nicht wiederverwendbare Eingabeobjekte hinzufügen möchten, müssen Sie eine persistente Eingabedatei verwenden, die kodierte Objekt-IDs enthält.

Wenn AddToDeploymentGroup erfolgreich ausgeführt wird, sendet der Befehl entweder keine Statusinformationen zurück oder er liefert eine Liste von Objekten, die bereits in der Bereitstellungsgruppe vorhanden sind. Wenn der Befehl fehlschlägt, zeigt er die Ursache des Fehlers an.

Der AddToDeploymentGroup-Befehl verwendet die folgende Syntax:

```
addtodeploymentgroup
-p <deployment_group_name>
{{-n <object_name>
-o <object_type>
-t <object_subtype>]
[-v <version_number>]
[-f <folder_name>]} |
[-i <persistent_input_file>]}
[-d <dependency_types (all, "non-reusable", or none)>]
[-s dbd_separator]
```

In der folgenden Tabelle werden *pmrep* AddToDeploymentGroup-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-p	deployment_group_name	Erforderlich. Name der Bereitstellungsgruppe, der Objekte hinzugefügt werden.
-n	object_name	Erforderlich beim Hinzufügen eines bestimmten Objekts. Name des Objekts, das Sie der Bereitstellungsgruppe hinzufügen. Der Name eines ausgecheckten Objekts kann nicht eingegeben werden. Bei Verwendung der Option -i kann die Option -n nicht benutzt werden.
-o	object_type	Erforderlich beim Hinzufügen eines bestimmten Objekts. Typ des Objekts, das Sie hinzufügen. Sie können Quelle, Target, Transformation, Mapping, Sitzung, Worklet, Arbeitsablauf, Scheduler, Sitzungskonfiguration, Aufgabe, Cube und Größenordnung festlegen.
-t	object_subtype	Erforderlich bei Verwendung gültiger Subtypen. Der Aufgaben- oder Transformationstyp, den Sie hinzufügen. Weitere Informationen zu gültigen Subtypen finden Sie unter <a href="#">"Listing Object Types" auf Seite 1494</a> .
-v	version_number	Optional. Version des hinzuzufügenden Objekts. Standard ist die neueste Version des Objekts. Der Befehl schlägt fehl, wenn Sie eine Versionsnummer für ein nicht versionsgesteuertes Repository angeben.
-f	folder_name	Erforderlich, wenn Sie einen Objektnamen eingeben. Ordner, der das hinzuzufügende Objekt enthält.
-i	persistent_input_file	Eine mit ExecuteQuery, Validate oder ListObjectDependencies generierte Textdatei, die eine Liste der Objektdatensätze mit kodierten IDs enthält. Wenn Sie diesen Parameter verwenden, lässt <i>pmrep</i> die Optionen -n, -o und -f nicht zu.

Option	Argument	Beschreibung
-d	dependency_types	<p>Optional. Abhängige Objekte, die der Bereitstellungsgruppe mit dem Objekt hinzugefügt werden können. Geben Sie einen der folgenden Parameter ein:</p> <ul style="list-style-type: none"> <li>- all. <i>pmrep</i> fügt die Objekte und alle abhängigen Objekte, sowohl wiederverwendbare als auch nicht wiederverwendbare, der Bereitstellungsgruppe hinzu.</li> <li>- "non-reusable". <i>pmrep</i> fügt die Objekte und die entsprechenden nicht wiederverwendbaren, abhängigen Objekte der Bereitstellungsgruppe hinzu.</li> <li>- Keine. <i>pmrep</i> fügt der Bereitstellungsgruppe keine abhängigen Objekte hinzu.</li> </ul> <p>Wenn Sie diesen Parameter auslassen, fügt <i>pmrep</i> die Objekte und alle abhängigen Objekte der Bereitstellungsgruppe hinzu.  <b>Hinweis:</b> Schließen Sie Argumente, die Leerzeichen oder nicht-alphanumerische Zeichen enthalten, in doppelte Anführungszeichen ein.</p>
-s	dbd_separator	<p>Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name\source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.</p>

## ApplyLabel

Wendet eine Beschriftung auf ein Objekt oder eine Reihe von Objekten in einem Ordner an. Wenn Sie einen Ordernamen eingeben, erhalten alle Objekte in diesem Ordner die Beschriftung. Sie können die Beschriftung auf abhängige Objekte anwenden. Wenn Sie die Option *dependency\_object\_types* verwenden, wendet *pmrep* die Beschriftung auf alle abhängigen Objekte an. Um eine Beschriftung auf ausgewählte abhängige Objekte anzuwenden, trennen Sie jeden Objekttypnamen in der Befehlszeile durch Komma ohne Leerzeichen ab.

Verwenden Sie ApplyLabel, um wiederverwendbare Eingabeobjekte zu beschriften. Wenn Sie nicht wiederverwendbare Eingabeobjekte beschriften möchten, müssen Sie eine persistente Eingabedatei verwenden, die kodierte Objekt-IDs enthält.

Wenn ApplyLabel erfolgreich ist, zeigt *pmrep* entweder keine Statusinformationen oder eine Liste von Objekten an, die bereits über die Beschriftung verfügen. Wenn der Befehl fehlschlägt, zeigt *pmrep* den Grund für den Fehler an.

Der ApplyLabel-Befehl verwendet die folgende Syntax:

```
applylabel
-a <label_name>
{{-n <object_name>
  -o <object_type>
    [-t <object_subtype>]
    [-v <version_number>]
    [-f <folder_name>] } |
-i <persistent_input_file>}
```

```

[-d <dependency_object_types>]

[-p <dependency_direction (children, parents, or both)>]

[-s (include pk-fk dependency)]

[-g (across repositories)]

[-m (move label)]

[-c <comments>]

[-e dbd_separator]

```

In der folgenden Tabelle werden *pmrep* ApplyLabel-Optionen und Argumente beschrieben:

Option	Argument	Beschreibung
-a	label_name	Erforderlich. Beschriftungsname, der auf das Objekt angewendet werden soll.
-n	object_name	Erforderlich, wenn Sie ein bestimmtes Objekt aktualisieren. Name des Objekts, das die Beschriftung erhalten soll. Sie können keine Objektamen eingeben, wenn Sie die Option -i verwenden.
-o	object_type	Typ des Objekts, auf das die Beschriftung angewendet werden soll. Sie können Quelle, Target, Transformation, Mapping, Sitzung, Worklet, Arbeitsablauf, Scheduler, Sitzungskonfiguration, Aufgabe, Cube oder Größenordnung festlegen. Erforderlich beim Anwenden einer Beschriftung auf ein bestimmtes Objekt.
-t	object_subtype	Erforderlich. Der Aufgaben- oder Transformationstyp, der beschriftet wird. <i>pmrep</i> ignoriert andere Objekttypen. Weitere Informationen zu gültigen Subtypen finden Sie unter <a href="#">"Listing Object Types" auf Seite 1494</a> .
-v	version_number	Optional. Version des Objekts, auf das die Beschriftung angewendet werden soll. Der Befehl schlägt fehl, wenn die Version ausgecheckt wurde. Wendet die Beschriftung standardmäßig auf die neueste Version an.
-f	folder_name	Optional. Ordner, der die Objekte enthält. Wenn Sie einen Ordernamen, jedoch keinen Objektamen eingeben, wendet <i>pmrep</i> die Beschriftung auf alle Objekte im Ordner an. Wenn Sie einen Ordernamen mit einem Objektamen eingeben, sucht <i>pmrep</i> in dem Ordner nach dem Objekt. Die Option -f kann nicht verwendet werden, wenn Sie die Option -i benutzen.
-i	persistent_input_file	Optional. Name einer Textdatei, die mit ExecuteQuery, ListObjectDependency oder Validate generiert wurde. Enthält eine Liste der Objekte, auf die die Beschriftung angewendet werden soll. Wenn Sie diese Option verwenden, dürfen Sie weder Objektamen, Objekttyp noch Ordernamen zur Angabe von Objekten verwenden.
-d	dependency_object_types	Optional. Zu beschriftende abhängige Objekttypen. Zu den gültigen abhängigen Objekttypen gehören Shortcuts, Mappings, Mapplets, Sitzungen, Arbeitsabläufe, Worklets, Target-Definitionen, Quelldefinitionen und Fremdschlüssel-Abhängigkeiten.  Verwenden Sie diese Option mit der Option -p. Wenn Sie einen Objekttyp eingeben, wird die Beschriftung auf abhängige Objekte dieses Objekttyp angewendet.

Option	Argument	Beschreibung
-p	dependency_direction	Optional. Über- oder untergeordnete abhängige Objekte, auf die die Beschriftung angewendet werden soll. Sie können übergeordnete oder untergeordnete Objekte bzw. beides festlegen. Wenn Sie die Option -d nicht eingeben, erhalten alle abhängigen Objekte die Beschriftung. Wenn Sie diese Option nicht eingeben, wird die Beschriftung auf das angegebene Objekt angewendet.
-s	-	Optional. Schließen Sie die Objekte mit Primärschlüssel-Fremdschlüssel-Abhängigkeiten unabhängig von der Abhängigkeitsrichtung ein.
-g	-	Optional. Suchen Sie nach Objektabhängigkeiten über Repositories.
-m	-	Optional. Verschieben Sie eine Beschriftung von der aktuellen Version auf die neueste Version eines Objekts. Verwenden Sie dieses Argument, wenn der Beschriftungstyp one_per_object lautet.
-c	Kommentare	Optional. Kommentare zur Beschriftung.
-e	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name \source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.

## AssignIntegrationService

Weist den PowerCenter-Integrationsdienst dem angegebenen Arbeitsablauf zu.

Wenn Sie den Arbeitsablauf über den Arbeitsablauf-Manager ausführen und dem Arbeitsablauf im Befehl *pmrep AssignIntegrationService* einen PowerCenter-Integrationsdienst zugeordnet haben, wird der Arbeitsablauf in dem in der Option -i angegebenen PowerCenter-Integrationsdienst ausgeführt.

Wenn Sie den Arbeitsablauf über die Befehlszeile ausführen, wird der Arbeitsablauf in dem im Befehl *pmcmd StartWorkflow* angegebenen PowerCenter-Integrationsdienst ausgeführt. Der Arbeitsablauf wird nicht in dem PowerCenter-Integrationsdienst ausgeführt, den Sie im Befehl *pmrep AssignIntegrationService* angegeben haben.

Für den Befehl „AssignIntegrationService“ wird die folgende Syntax verwendet:

```
assignintegrationsservice
-f <folder_name>
-n <workflow_name>
-i <integration_service_name>
```

In der folgenden Tabelle werden die Optionen und Argumente für *pmrep* AssignIntegrationService beschrieben:

Option	Argument	Beschreibung
-f	folder_name	Erforderlich. Name des Ordners, der den Arbeitsablauf enthält. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-n	workflow_name	Erforderlich. Name des Arbeitsablaufs.
-i	integration_service_name	Erforderlich. Name des PowerCenter-Integrationsdiensts für den Arbeitsablauf.

## AssignPermission

Ermöglicht das Hinzufügen, Entfernen oder Aktualisieren von Berechtigungen bei einem globalen Objekt für einen Benutzer, eine Gruppe oder die Standardgruppe "Andere".

**Hinweis:** Nur der Administrator oder der aktuelle Eigentümer des Objekts kann Berechtigungen für das Objekt verwalten.

Der AssignPermission-Befehl verwendet die folgende Syntax:

```
AssignPermission
-o <object_type>
[-t <object_subtype>]
-n <object_name>
{-u <user_name> | -g <group_name>}
[-s <security_domain>]
-p <permission>
```

In der folgenden Tabelle werden *pmrep* AssignPermission-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	object_type	Erforderlich. Typ des Objekts, für das Sie Berechtigungen verwalten möchten. Sie können Ordner, Beschriftung, Bereitstellungsgruppe, Abfrage oder Verbindung festlegen.
-t	object_subtype	Optional. Typ des Verbindungsobjekts oder der Abfrage. Nicht erforderlich für andere Objekttypen. Weitere Informationen zu gültigen Subtypen finden Sie unter <a href="#">"AssignPermission" auf Seite 1452</a> .
-n	object_name	Erforderlich. Name des Objekts, für das Sie Berechtigungen verwalten möchten. Sie können Sonderzeichen für den Objektamen verwenden.



Option	Argument	Beschreibung
-u	user_name	Erforderlich, wenn Sie nicht die Option -g verwenden. Name des Benutzers, für den Sie Berechtigungen hinzufügen, entfernen oder aktualisieren möchten. Verwenden Sie die Option -u oder die Option -g, nicht beide.
-g	group_name	Name der Gruppe, für die Sie Berechtigungen hinzufügen, entfernen oder aktualisieren möchten. Geben Sie „Andere“ als Gruppenname an, um Berechtigungen der Standardgruppe „Andere“ zu ändern. Verwenden Sie die Option -u oder die Option -g, aber nicht beide. Sie können Sonderzeichen für den Gruppennamen verwenden.
-s	security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer oder die Gruppe gehört. Standardwert ist „Native“.
-p	permission	Erforderlich. Berechtigungen, die Sie hinzufügen, entfernen oder aktualisieren möchten. Sie weisen Lese-, Schreib- und Ausführungsberechtigungen einem globalen Objekt zu. Verwenden Sie die Zeichen r, w und x, um Lese-, Schreib- und Ausführungsberechtigungen zuzuweisen.

In der folgenden Tabelle werden die Objekttypen und Werte beschrieben, die bei den *pmrep*-Befehlen verwendet werden:

Objekttyp	Objekt-Subtyp
Abfrage	Gemeinsam genutzt
Abfrage	Persönlich
Verbindung	Anwendung
Verbindung	FTP
Verbindung	Loader
Verbindung	Warteschlange
Verbindung	Relational

## Beispiel

Sie können Berechtigungen mit der Option -p hinzufügen, entfernen oder aktualisieren.

Um beispielsweise Lese- und Schreibberechtigungen für einen Ordner hinzuzufügen, geben Sie den folgenden Text bei der Eingabeaufforderung ein:

```
pmrep AssignPermission -o folder -n Sales -u Admin -p rw
```

Sie können Berechtigungen für ein Objekt auch aktualisieren. Beispiel: Sie haben einem Ordner eine Leseberechtigung zugewiesen und müssen nun auch die Schreibberechtigung zuweisen. Geben Sie zum Aktualisieren von Berechtigungen den folgenden Text bei der Eingabeaufforderung ein:

```
pmrep AssignPermission -o folder -n Sales -u Admin -p rw
```

Um alle Berechtigungen zu entfernen, geben Sie den folgenden Text bei der Eingabeaufforderung ein:

```
pmrep AssignPermission -o folder -n Sales -u Admin -p ""
```

## BackUp

Sichert das Repository in die mit der Option -o angegebene Datei. Sie müssen der Backup-Datei einen Namen zuweisen. Verwenden Sie diesen Befehl, wenn das Repository ausgeführt wird. Sie müssen mit einem Repository verbunden sein, um diesen Befehl verwenden zu können.

Der BackUp-Befehl verwendet die folgende Syntax:

```
backup  
  
-o <output_file_name>  
  
[-d <description>]  
  
[-f (overwrite existing output file)]  
  
[-b (skip workflow and session logs)]  
  
[-j (skip deploy group history)]  
  
[-q (skip MX data)]  
  
[-v (skip task statistics)]
```

In der folgenden Tabelle werden die *pmrep* Backup-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	output_file_name	Erforderlich. Name und Pfad der Datei für die Repository-Sicherung. Wenn Sie die Liste der Repository-Backup-Dateien im Administrator-Tool anzeigen, werden nur Dateien mit der Erweiterung .rep aufgeführt.
-d	Beschreibung	Optional. Erstellt eine Beschreibung der Backup-Datei basierend auf der Zeichenfolge, die der Option folgt. Beim Sicherungsprozess werden alle Zeichenfolgen nach 2.000 Zeichen trunziert.
-f	-	Optional. Überschreibt eine vorhandene Datei mit demselben Namen.
-b	-	Optional. Überspringt während des Backups Tabellen, die sich auf Arbeitsablauf und Sitzungsprotokolle beziehen.
-j	-	Optional. Überspringt während des Backup die Bereitstellungsgruppen-Historie.
-q	-	Optional. Überspringt während des Backups Tabellen, die sich auf MX-Daten beziehen.
-v	-	Optional. Überspringt während des Backups Aufgabenstatistiken.

Verwenden Sie zum Wiederherstellen der Backup-Datei das Administrator-Tool oder den Befehl *pmrep* Restore.

# ChangeOwner

Ändert den Namen des Eigentümers für ein globales Objekt.

**Hinweis:** Nur der Administrator oder der aktuelle Eigentümer des Objekts darf den Eigentümer eines Objekts ändern.

Der ChangeOwner-Befehl verwendet die folgende Syntax:

```
ChangeOwner  
-o <object_type>  
[-t <object_subtype>]  
-n <object_name>  
-u <new_owner_name>  
[-s <security_domain>]
```

In der folgenden Tabelle werden die *pmrep* ChangeOwner-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	object_type	Erforderlich. Typ des Objekts. Sie können Ordner, Beschriftung, Bereitstellungsgruppe, Abfrage oder Verbindung festlegen.
-t	object_subtype	Optional. Typ der Objektabfrage oder des Verbindungsobjekts. Nicht erforderlich für andere Objekttypen. Weitere Informationen zu gültigen Subtypen finden Sie unter <a href="#">"AssignPermission" auf Seite 1452</a> .
-n	object_name	Erforderlich. Name des Objekts Sie können Sonderzeichen für den Objektnamen verwenden.
-u	new_owner_name	Erforderlich. Name des geänderten Eigentümers. Der geänderte Eigentümername muss ein gültiges Benutzerkonto in der Domäne sein.
-s	security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der neue Eigentümer gehört. Standardwert ist „Native“.

# CheckIn

Checkt ein Objekt ein, das Sie ausgecheckt haben. Wenn Sie ein Objekt einchecken, erstellt das Repository eine neue Version des Objekts und weist ihm eine Versionsnummer zu. Die Versionsnummer ist um eine Zahl höher als die Versionsnummer der letzten eingetragenen Version.

Der CheckIn-Befehl verwendet die folgende Syntax:

```
checkin  
-o <object_type>  
[-t <object_subtype>]  
-n <object_name>  
-f <folder_name>
```

```
[-c <comments>]
```

```
[-s dbd_separator]
```

In der folgenden Tabelle werden die *pmrep* CheckIn-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	object_type	Erforderlich. Typ des einzucheckenden Objekts: Quelle, Target, Transformation, Mapping, Sitzung, Worklet, Arbeitsablauf, Scheduler, Sitzungskonfiguration, Aufgabe, Cube oder Größenordnung.
-t	object_subtype	Optional. Der Typ der einzuscheckenden Aufgabe oder Transformation. Nicht erforderlich für andere Objekttypen. Weitere Informationen zu gültigen Subtypen finden Sie unter <a href="#">"Listing Object Types" auf Seite 1494</a> .
-n	object_name	Erforderlich. Name des einzucheckenden Objekts.
-f	folder_name	Erforderlich. Ordner, in dem die neue Objektversion gespeichert werden soll.
-c	Kommentare	Optional. Kommentare zum Einchecken.
-s	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name\source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.

## CleanUp

Bereinigt alle von *pmrep* erstellten persistenten Ressourcen. Dieser Befehl bereinigt auch alle Verbindungsinformationen aus vorherigen Sitzungen von *pmrep*. Wird CleanUp in einer Sitzung als erster Befehl aufgerufen, führt dies immer zu einem Fehler.

Wenn Sie CleanUp im interaktiven Modus aufrufen, trennt *pmrep* alle verbundenen Repositories.

Der CleanUp-Befehl verwendet die folgende Syntax:

```
cleanup
```

## ClearDeploymentGroup

Löscht alle Objekte aus einer Bereitstellungsgruppe. Verwenden Sie diesen Befehl, um die Bereitstellungsgruppe zu behalten und die Objekte zu entfernen.

Der ClearDeploymentGroup-Befehl verwendet die folgende Syntax:

```
cleardeploymentgroup  
-p <deployment_group_name>  
[-f (force clear)]
```

In der folgenden Tabelle werden die *pmrep* ClearDeploymentGroup- Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-p	deployment_group_name	Erforderlich. Name der Bereitstellungsgruppe, die Sie löschen möchten.
-f	-	Optional. Entfernen Sie Objekte ohne Bestätigung. Wenn Sie dieses Argument auslassen, werden Sie aufgefordert, das Löschen der Objekte zu bestätigen.

## Connect

Stellt die Verbindung zu einem Repository her. Wenn Sie *pmrep* in der Befehlszeile oder im interaktiven Modus zum ersten Mal benutzen, müssen Sie den Connect-Befehl verwenden. Alle Befehle erfordern eine Verbindung zum Repository. Davon ausgenommen sind folgende Befehle:

- Exit
- Hilfe
- ListAllPrivileges

Im Befehlszeilenmodus verwendet *pmrep* die Informationen, die beim letzten Verbindungsaufruf zum Repository verwendet wurden. Wenn *pmrep* ohne erfolgreiche Verbindung aufgerufen wird, führt dies zu einem Fehler. In Befehlszeilenmodus stellt *pmrep* bei jedem Befehl eine Verbindung zum Repository her und trennt diese wieder.

Um *pmrep* zur Ausführung von Aufgaben in mehreren Repositories in einer einzigen Sitzung zu verwenden, müssen Sie den Connect-Befehl jedes Mal ausführen, wenn Sie zu einem anderen Repository wechseln möchten. Im interaktiven Modus behält *pmrep* die Verbindung bei, bis Sie *pmrep* beenden oder eine neue Verbindung herstellen. Wenn Sie Connect erneut aufrufen, trennt *pmrep* die Verbindung zum ersten Repository und stellt dann eine Verbindung zum zweiten Repository her. Wenn die zweite Verbindung fehlschlägt, bleibt die vorhergehende Verbindung weiterhin getrennt, sodass keine Verbindung zu einem Repository besteht. Wenn Sie einen Befehl ausführen, der eine Verbindung zum Repository benötigt, und Sie nicht mit diesem Repository verbunden sind, verwendet *pmrep* die Verbindungsinformationen der letzten erfolgreichen Verbindung zum Repository aus einer früheren Sitzung von *pmrep*. *pmrep* behält Informationen aus der letzten erfolgreichen Verbindung bei, bis Sie den Cleanup-Befehl verwenden.

Der Befehl „Connect“ verwendet die folgende Syntax:

```
connect
-r <repository_name>
{-d <domain_name> |
  {-h <portal_host_name>
    -o <portal_port_number>}}
[{-n <user_name>
  -s <user_security_domain>
  -x <password> |
    -X <password_environment_variable>}] |
-u <connect_without_user_in_kerberos_mode>]
```

`[-t <client_resilience>]`

In der folgenden Tabelle werden die Optionen und Argumente für „pmrep Connect“ beschrieben:

Option	Argument	Beschreibung
-r	repository_name	Erforderlich. Name des Repositorys, zu dem Sie eine Verbindung herstellen möchten.
-d	domain_name	Erforderlich, wenn Sie nicht -h und -o verwenden. Der Name der Domäne für das Repository. Wenn Sie die Option -d verwenden, dürfen Sie nicht die Optionen -h und -o benutzen.
-h	portal_host_name	Erforderlich, wenn Sie nicht -d verwenden. Wenn Sie die Option -h benutzen, müssen Sie auch die Option -o verwenden. Gateway-Hostname.
-o	portal_port_number	Erforderlich, wenn Sie nicht -d verwenden. Wenn Sie die Option -o verwenden, müssen Sie auch die Option -h verwenden. Gateway-Portnummer.
-n	user_name	Optional. Benutzername zum Herstellen einer Verbindung zum Repository.
-s	user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Der Standardwert ist „Nativ“.
-x	password	Erforderlich, wenn Sie die Option -n und nicht die Option -X verwenden. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Verwenden Sie die Option -x oder -X, aber nicht beide.
-X	password_environment_variable	Erforderlich, wenn Sie die Option -n und nicht die Option -x verwenden. Umgebungsvariable für das Passwort. Verwenden Sie die Option -x oder -X, aber nicht beide.

Option	Argument	Beschreibung
-u	connect_without_user_ in_kerberos_mode	Erforderlich. Stellt eine Verbindung zu einem Repository-Dienst ohne Benutzernamen und Passwort her, wenn die Informatica-Domäne die Kerberos-Authentifizierung verwendet. Verwenden Sie die Option -u, um eine Verbindung zum Repository-Dienst herzustellen, wenn das Repository keinen Inhalt hat.
-t	client_resilience	Optional. Zeit (in Sekunden), in der pmrep versucht, eine Verbindung zum Repository herzustellen bzw. erneut herzustellen. Wenn Sie die Option -t auslassen, verwendet pmrep den Timeout-Wert, der in der INFA_CLIENT_RESILIENCE_TIMEOUT-Umgebungsvariablen angegeben ist. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

## Create

Erstellt die Repository-Tabellen in der Datenbank. Bevor Sie die Repository-Tabellen erstellen können, müssen Sie diese Aufgaben abschließen:

- Erstellen und konfigurieren Sie die Datenbank, die das Repository enthalten soll.
- Erstellen Sie den Repository Service im Administrator-Tool oder in *infacmd*.
- Führen Sie den Repository Service im exklusiven Modus im Administrator-Tool oder in *infacmd* aus.
- Stellen Sie eine Verbindung zum Repository in *pmrep* her.

Der Create-Befehl kann nicht verwendet werden, wenn die Repository-Datenbank bereits Repository-Tabellen enthält.

Um den Create-Befehl zu verwenden, müssen Sie über die Berechtigung für den Repository Service in der Domäne verfügen.

Der Create-Befehl verwendet die folgende Syntax:

```
create
-u <domain_user_name>
[-s <domain_user_security_domain>]
[-p <domain_password> |
-P <domain_password_environment_variable>]
[-g (create global repository)]
[-v (enable object versioning)]
```

In der folgenden Tabelle werden die *pmrep* Create-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-u	domain_user_name	Erforderlich. Benutzername.
-s	domain_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Die Standardeinstellung ist "Native".
-p	domain_password	Optional. Passwort. Verwenden Sie entweder die Option -p oder -P, aber nicht beide. Wenn Sie weder die Option -p noch -P verwenden, werden Sie von <i>pmrep</i> aufgefordert, das Passwort einzugeben.
-P	domain_password_environment_variable	Optional. Passwort-Umgebungsvariable. Verwenden Sie entweder die Option -p oder -P, aber nicht beide. Wenn Sie weder die Option -p noch -P verwenden, werden Sie von <i>pmrep</i> aufgefordert, das Passwort einzugeben.
-g	-	Optional. Stuft das Repository zu einem globalen Repository hoch.
-v	-	Optional. Ermöglicht die Objektversionierung für das Repository.

## CreateConnection

Erstellt eine Quell- oder Target-Verbindung im Repository. Die Verbindung kann eine relationale, Anwendungs- oder FTP-Verbindung sein. Relationale Datenbankverbindungen für alle relationalen Subtypen benötigen eine Teilmenge aller CreateConnection-Optionen und -Argumente. Zum Beispiel werden die Optionen -z, -d oder -t von Oracle-Verbindungen nicht akzeptiert. Verwenden Sie die Option -k zum Festlegen der Attribute für Anwendungsverbindungen.

Der Befehl „CreateConnection“ verwendet die folgende Syntax:

```
createconnection
-s <connection_subtype>
-n <connection_name>
[{-u <user_name>
  [-p <password> |
    -P <password_environment_variable>
    [-w (use parameter in password)]]]]
-K <connection_to_the_Kerberos_server>
[-c <connect_string> (required for Oracle, Informix, DB2, Microsoft SQL Server, ODBC,
and NetezzaRelational)]
[-l <code_page>]
[-r <rollback_segment> (valid for Oracle connection only)]
[-e <connection_environment_SQL>]
[-f <transaction_environment_SQL>]
```



```

[-z <packet_size> (valid for Sybase ASE and MS SQL Server connection)]

[-b <database_name> (valid for Sybase ASE, Teradata and MS SQL Server connection)]

[-v <server_name> (valid for Sybase ASE and MS SQL Server connection)]

[-d <domain_name> (valid for MS SQL Server connection only)]

[-t (enable trusted connection, valid for MS SQL Server connection only)]

[-a <data_source_name> (valid for Teradata connection only)]

[-x (enable advanced security, lets users give Read, Write and Execute permissions only
for themselves.)]

[-k <connection_attributes> (attributes have the format name=value;name=value; and so
on)]

[-y (Provider Type (1 for ODBC and 2 for OLEDB), valid for MS SQL Server connection
only)]

[-m (UseDSN, valid for MS SQL Server connection only)]

[-S <odbc_subtype> (valid for ODBC connection only, default is None)]

```

In der folgenden Tabelle werden die Optionen und Argumente für „*pmrep* CreateConnection“ beschrieben:

Option	Argument	Beschreibung
-s	connection_subtype	<p>Erforderlich. Zeigt den Verbindungsuntertyp an.  Folgende Verbindungstypen sind möglich:</p> <ul style="list-style-type: none"> <li>- Anwendung</li> <li>- FTP</li> <li>- Relational</li> </ul> <p>Bei einer relationalen Verbindung gehören zu den Verbindungssubtypen beispielsweise Oracle, Sybase und Microsoft SQL Server. Der gültige Subtyp für FTP-Verbindungen ist FTP.</p>
-n	connection_name	Erforderlich. Name der Verbindung.
-u	user_name	Für bestimmte Verbindungstypen erforderlich. Für die Authentifizierung verwendeter Benutzername.
-p	password	<p>Für bestimmte Verbindungstypen erforderlich. Passwort für die Authentifizierung beim Herstellen einer Verbindung zur relationalen Datenbank. Verwenden Sie die Option -p oder -P, aber nicht beide. Wenn Sie einen Benutzernamen angeben, aber weder -p noch -P verwenden, werden Sie von <i>pmrep</i> zur Eingabe des Passworts aufgefordert.</p> <p>Um im Passwort einen Parameter anzugeben, fügen Sie das Präfix „\$Param“ für die Option -p hinzu, und stellen Sie sicher, dass Sie die Option -w verwenden. Verwenden Sie das Dollarzeichen (\$) ausschließlich in der Option -p und geben Sie das Parameterpasswort ohne Leerzeichen ein. Beispiel: -p '\$Param_abc' -w</p>
-P	password_environment_variable	<p>Optional. Passwort-Umgebungsvariable für die Authentifizierung, wenn Sie eine Verbindung zu der relationalen Datenbank herstellen. Verwenden Sie die Option -p oder -P, aber nicht beide. Wenn Sie weder die Option -p noch -P verwenden, werden Sie von <i>pmrep</i> zur Eingabe des Passworts aufgefordert.</p>

Option	Argument	Beschreibung
-w	-	Optional. Ermöglicht es Ihnen, einen Parameter in der Passwortoption zu verwenden. <i>pmrep</i> verwendet das mit der Option -p oder -P angegebene Passwort als Namen des Sitzungsparameters zur Laufzeit. Nur gültig, wenn Sie die Option -p oder -P verwenden. Wenn Sie in der Passwortoption keinen Parameter festlegen, verwendet <i>pmrep</i> das mit der Option -p oder -P angegebene Benutzerpasswort.
-K	connection_to_the_Kerberos_server	Optional. Gibt an, dass die Datenbank, zu der Sie eine Verbindung herstellen, in einem Netzwerk ausgeführt wird, das die Kerberos-Authentifizierung verwendet.
-c	connect_string	Verbindungszeichenfolge, die der Integrationsdienst verwendet, um eine Verbindung zur relationalen Datenbank herzustellen.
-l	code_page	Für bestimmte Verbindungstypen erforderlich. Codepage, die der Verbindung zugeordnet ist.
-r	rollback_segment	Optional. Gültig für Oracle-Verbindungen. Der Name des Rollbacksegments. Datenbanktransaktionen mit Rollbacksegment-Datensätzen, mit denen Sie die Transaktion rückgängig machen können.
-e	connection_environment_sql	Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Integrationsdienst führt die Verbindungsumgebungs-SQL bei jeder Verbindungsherstellung mit der Datenbank aus.
-f	transaction_environment_sql	Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Integrationsdienst führt die Transaktionsumgebungs-SQL am Anfang jeder Transaktion aus.
-z	packet_size	Optional. Gültig für Sybase ASE- und Microsoft SQL Server-Verbindungen. Optimiert die ODBC-Verbindung zu Sybase ASE und Microsoft SQL Server.
-b	database_name	Optional. Name der Datenbank. Gültig für Sybase ASE- und Microsoft SQL Server-Verbindungen.
-v	server_name	Optionaler Name des Datenbankservers. Gültig für Sybase ASE- und Microsoft SQL Server-Verbindungen.
-d	domain_name	Optional gültig für Microsoft SQL Server-Verbindungen. Der Name der Domäne. Verwendet für Microsoft SQL Server.
-t	-	Optional. Gültig für Microsoft SQL Server-Verbindungen. Bei Aktivierung verwendet der Integrationsdienst Windows-Authentifizierung, um auf die Microsoft SQL Server-Datenbank zuzugreifen. Der Name des Benutzers, der den Integrationsdienst startet, muss ein gültiger Windows-Benutzer mit Zugriff auf die Microsoft SQL Server-Datenbank sein.
-a	data_source_name	Optionaler Name der Teradata-ODBC-Datenquelle. Gültig für Teradata-Verbindungen.

Option	Argument	Beschreibung
-x	-	Aktiviert erweiterte Sicherheit. Gewährt Ihnen Berechtigungen zum Lesen, Schreiben und Ausführen. Öffentlichen und weltweiten Gruppen werden keine Berechtigungen gewährt. Wenn diese Option nicht aktiviert ist, werden allen Gruppen und Benutzern Lese-, Schreib- und Ausführungsberechtigungen gewährt.
-k	connection_attributes	Aktiviert benutzerdefinierte Verbindungsattribute. Attribute weisen das Format <name>=<value>;<name>=<value> auf. <b>Hinweis:</b> Fügen Sie vor dem Attributnamen kein Leerzeichen hinzu.
-y	-	Aktiviert den Wert des Providertyps. Sie können die folgenden Providertypen angeben: - 1 für ODBC - 2 für Oledb (Veraltet)
-m	-	Aktiviert das Attribut „DSN verwenden“. Der PowerCenter-Integrationsdienst ruft die Datenbank- und Servernamen aus dem DSN ab.
-S	odbc_subtype	Optional. Aktiviert den ODBC-Untertyp für eine ODBC-Verbindung. Eine ODBC-Verbindung kann einen der folgenden ODBC-Untertypen aufweisen: - AWS Redshift - Azure DW - Greenplum - Google Big Query - PostgreSQL - Snowflake - SAP HANA - Kein Standardwert ist „Kein“.

Weitere Informationen über Verbindungsuntertypen finden Sie unter [“Verbindungsuntertypen” auf Seite 1445](#).

## Festlegen der Datenbank-Codepage

Die Option -I gibt die Codepage für die Datenbankverbindung an. Geben Sie den Namen der Codepage ein, den Sie der Datenbankverbindung zuweisen möchten. Um beispielsweise die US-ASCII-Codepage der Datenbankverbindung zuzuweisen, geben Sie den Codepage-Namen "US-ASCII" ein

Das Ändern der Datenbankverbindungs-Codepage kann zu Dateninkonsistenzen führen, wenn die neue Codepage nicht mit den Codepages der Quell- oder Target-Datenbankverbindung kompatibel ist. Auch wenn Sie den Integration Service für die Datenvalidierung der Codepage konfigurieren, kann das Ändern der Datenbankverbindungs-Codepage zu einem Fehlschlagen von Sitzungen führen, wenn die Codepage der Quelldatenbank-Verbindung nicht Teil der Codepage der Target-Datenbankverbindung ist.

# CreateDeploymentGroup

Erstellt eine Bereitstellungsgruppe. Sie können eine dynamische oder statische Bereitstellungsgruppe erstellen. Zum Erstellen einer dynamischen Bereitstellungsgruppe müssen Sie einen Abfragenamen zur Verfügung stellen und angeben, ob es sich um eine private oder öffentliche Abfrage handelt.

Der CreateDeploymentGroup-Befehl verwendet die folgende Syntax:

```
createdeploymentgroup
-p <deployment_group_name>
[-t <deployment_group_type (static or dynamic)>]
[-q <query_name>]
[-u <query_type (shared or personal)>]
[-c <comments>]
```

In der folgenden Tabelle werden die *pmrep* CreateDeploymentGroup-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-p	deployment_group_name	Erforderlich. Der Name der zu erstellenden Bereitstellungsgruppe.
-t	deployment_group_type	Optional. Erstellen Sie eine statische Gruppe, oder verwenden Sie eine Abfrage zum dynamischen Erstellen der Gruppe. Sie können statisch oder dynamisch angeben. Der Standardwert ist statisch.
-q	query_name	Erforderlich, wenn die Bereitstellungsgruppe dynamisch ist. Wird jedoch ignoriert, wenn die Gruppe statisch ist. Name der Abfrage, die der Bereitstellungsgruppe zugeordnet ist.
-u	query_type	Erforderlich, wenn die Bereitstellungsgruppe dynamisch ist. Wird jedoch ignoriert, wenn die Gruppe statisch ist. Typ der Abfrage zum Erstellen einer Bereitstellungsgruppe. Sie können die gemeinsame oder persönliche Nutzung festlegen.
-c	Kommentare	Optional. Kommentare zu der neuen Bereitstellungsgruppe.

# CreateFolder

Erstellt einen Ordner im Repository.

Der CreateFolder-Befehl verwendet die folgende Syntax:

```
createfolder
-n <folder_name>
[-d <folder_description>]
[-o <owner_name>]
[-a <owner_security_domain>]
[-s (shared_folder)]
```

```
[-p <permissions>]
```

```
[-f <active | frozendeploy | frozennodeploy>]
```

In der folgenden Tabelle werden die *pmrepCreateFolder*-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-n	folder_name	Erforderlich. Ordnername.
-d	folder_description	Optional. Beschreibung des Ordners, der im Repository Manager angezeigt wird. Wenn die Ordnerbeschreibung Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen.
-o	owner_name	Optional. Eigentümer des Ordners. Jeder Benutzer im Repository kann Eigentümer des Ordners sein. Der Standardeigentümer ist der Benutzer, der den Ordner erstellt hat.
-a	owner_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Eigentümer gehört. Standardwert ist "Native".
-s	-	Optional. Stellt den Ordner zur gemeinsamen Nutzung zur Verfügung.
-p	Berechtigungen	Optional. Zugriffsberechtigungen für den Ordner. Wenn dies ausgelassen wird, weist der Repository Service Standardberechtigungen zu.
-f	active frozendeploy frozennodeploy	Optional. Ändert den Ordnerstatus auf einen der folgenden Status: <ul style="list-style-type: none"><li>- active. Dieser Status ermöglicht Benutzern das Auschecken versionsgesteuerter Objekte im Ordner.</li><li>- frozendeploy (Eingefroren, Ersetzen bei Bereitstellung zulassen). Dieser Status verhindert, dass Benutzer Objekte im Ordner auschecken. Bei der Bereitstellung im Ordner werden neue Versionen der Objekte erstellt.</li><li>- frozennodeploy (Eingefroren, Ersetzen bei Bereitstellung nicht zulassen). Dieser Status verhindert, dass Benutzer Objekte im Ordner auschecken. Sie können in diesem Ordner keine Objekte bereitstellen.</li></ul>

**Hinweis:** Mit dem AssignPermission-Befehl können Sie in einem Ordner Berechtigungen hinzufügen, entfernen oder aktualisieren.

## Zuweisen von Berechtigungen

Sie können Eigentümer-, Gruppen- und Repository-Berechtigungen durch Eingabe von drei Ziffern zuweisen, wenn Sie die Option -p verwenden. Die erste Ziffer entspricht den Eigentümerberechtigungen, die zweite entspricht den Berechtigungen der Gruppe, der der Benutzer angehört, und die dritte bezieht sich auf alle anderen Berechtigungen.

Geben Sie für jeden Berechtigungssatz eine Zahl ein. Jede Berechtigung ist einer Zahl zugeordnet. Verwenden Sie 4 für Leseberechtigung, 2 für Schreibberechtigung und 1 für Ausführungsberechtigung. Um Berechtigungen zuweisen, geben Sie 4, 2, 1 oder die Summe der entsprechenden Zahlen ein.

Wenn Sie beispielsweise Standardberechtigungen zuweisen möchten, verwenden Sie die folgende Befehlssyntax:

```
-p 764
```

Mit dieser Syntax erhält der Ordneigentümer die Berechtigung zum Lesen, Schreiben und Ausführen (7 = 4+2+1). Die Gruppe des Eigentümers hat Lese- und Schreibberechtigungen (6 = 4+2). Alle anderen haben Leseberechtigung.

Der Befehl gibt die Meldung "createfolder erfolgreich abgeschlossen" oder "createfolder fehlgeschlagen" zurück. Die Erstellung schlägt möglicherweise aus folgenden Gründen fehl:

- Der Ordner ist bereits vorhanden.
- Der Eigentümer existiert nicht oder gehört nicht zur Gruppe.

## CreateLabel

Erstellt eine Beschriftung, die Sie zum Zuordnen von Objektgruppen während der Entwicklung verwenden. Sie können eine Beschriftung jedem versionsgesteuerten Objekt bzw. jeder Objektgruppe in einem Repository zuordnen.

Der CreateLabel-Befehl verwendet die folgende Syntax:

```
createlabel  
-a <label_name>  
[-c <comments>]
```

In der folgenden Tabelle werden die *pmrep* CreateLabel-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-a	label_name	Erforderlich. Name der Beschriftung, die Sie erstellen.
-c	Kommentare	Optional. Kommentare zur Beschriftung.

## CreateQuery

Creates an object query in the repository. You must configure the query conditions to create an object query. A query condition consists of a parameter, an operator, and a value. You can enter the expression in a file or at the command prompt.

The CreateQuery command uses the following syntax:

```
createquery  
-n <query_name>  
-t <query_type (shared or personal)>  
{-e <expression> |  
-f <file_name>}  
[-u (UTF-8 encoded input file)]  
[-c <comments>]
```

The following table describes *pmrep* CreateQuery options and arguments:

Option	Argument	Description
-n	query_name	Required. Name of the query that you want to create.
-t	query_type	Required. The type of query. You can specify shared or personal.
-e	expression	Required if you do not use the -f option. Expression of the query.
-f	file_name	Required if you do not use the -e option. Name and path of the file that contains the expression of a query. You must use the -e or -f option, but not both.
-u	-	Optional. Encodes the file in the UTF-8 format. <b>Note:</b> If you do not specify the -u option, the default system encoding encodes the file.
-c	comments	Optional. Comments about the query.

The following table describes the query parameters and the valid operators and values for each parameter that you can use in an expression:

Parameter	Description	Valid Operator	Accepted Values
BusinessName	Displays sources and targets based on their business names. For example, the query Business Name is Equal to Informatica, returns sources and targets that contain the Informatica business name and filters out all other objects.	Contains, EndsWith, Equals, In, Not Contains, Not Equals, Not EndsWith, Not In, Not StartsWith, StartsWith	String
CheckinTime	Displays checked in versioned objects for a specified time, before or after a specified time, or within a specified number of days. You can specify this parameter for versioned repositories only.	Between, GreaterThan, LessThan, Not Between, WithinLastDays	Date/time, Numeric
CheckoutTime	Displays checked out versioned objects for a specified time, before or after a specified time, or within a specified number of days. You can specify this parameter for versioned repositories only.	Between, GreaterThan, LessThan, Not Between, WithinLastDays	Date/time, Numeric

Parameter	Description	Valid Operator	Accepted Values
Comments	Displays comments associated with a source, target, mapping, or workflow.	Contains, Equals, EndsWith, In, Not Contains, Not Equals, Not EndsWith, Not In, Not StartsWith, StartsWith	String
DeploymentDispatchHistory	Displays versioned objects deployed to another folder or repository through deployment groups in a given time period.	Between, GreaterThan, LessThan, Not Between, WithinLastDays	Date/time, Numeric
DeploymentReceiveHistory	Displays versioned objects deployed from another folder or repository using deployment groups in a given time period.	Between, GreaterThan, LessThan, Not Between, WithinLastDays	Date/time, Numeric
Folder	Displays objects in a specified folder.	Equals, In, Not Equals, Not In	Folder name



Parameter	Description	Valid Operator	Accepted Values
IncludeChildren	Displays child dependent objects.	Where (Value 1) depends on (Value 2), (Value 3)	For value 1 and value 2, use: Any, Source Definition, Target Definition, Transformation, Mapplet, Mapping, Cube, Dimension, Task, Session, Worklet, Workflow, Scheduler, SessionConfig For value 3 use: Non-reusable dependency, Reusable dependency.
IncludeChildrenAndParents	Displays child and parent dependent objects.	Where (Value 1) depends on (Value 2), (Value 3)	For value 1 and value 2, use: Any, Source Definition, Target Definition, Transformation, Mapplet, Mapping, Cube, Dimension, Task, Session, Worklet, Workflow, Scheduler, SessionConfig For value 3 use: Non-reusable dependency, Reusable dependency.

Parameter	Description	Valid Operator	Accepted Values
IncludeParents	Displays parent dependent objects.	Where (Value 1) depends on (Value 2), (Value 3)	For value 1 and value 2, use: Any, Source Definition, Target Definition, Transformation, Mapplet, Mapping, Cube, Dimension, Task, Session, Worklet, Workflow, Scheduler, SessionConfig For value 3 use: Non-reusable dependency, Reusable dependency.
IncludePKFKDependencies	Displays primary key-foreign key dependencies.	-	-
ImpactedStatus	Displays objects based on impacted status. Objects can be marked as impacted when a child object changes in such a way that the parent object may not be able to run.	Equals	Impacted, Not Impacted
Label	Displays versioned objects associated with a label or group of labels. You can specify this parameter for versioned repositories only.	Contains, Equals, EndsWith, In, Not Contains, Not Equals, Not EndsWith, In, Not StartsWith, Not In, StartsWith	String
LastSavedTime	Displays objects saved at a particular time or within a particular time range.	Between, GreaterThan, LessThan, Not Between, WithinLastDays	Date/time, Numeric

Parameter	Description	Valid Operator	Accepted Values
LatestStatus	Displays versioned objects based on the object history. The query can return local objects that are checked out, the latest version of checked-in objects, or a collection of all older versions of objects. You can specify this parameter for versioned repositories only.	Equals, Not Equals, In	Checked-out Latest, Checked-in Older
MetadataExtension	Displays objects based on an extension name or value pair. Use this query parameter to find non-reusable metadata extensions. The query does not return user-defined reusable metadata extensions.	Equals, Not Equals	Vendor-defined metadata domain
ObjectName	Displays objects based on the object name.	Contains, Equals, EndsWith, In, Not Contains, Not Equals, Not EndsWith, Not StartsWith, Not In, StartsWith	String
ObjectType	Displays objects based on the object type. For example, you can find all workflows in a specified folder.	Equals, In, Not Equals, Not In	Cube, Dimension, Mapping, Mapplet, Scheduler, Session, Session Config, Source Definition, Target Definition, Task, Transformation, User-Defined Function, Workflow, Worklet

Parameter	Description	Valid Operator	Accepted Values
ObjectUsedStatus	Displays objects that are used by other objects. For example, you can find mappings that are not used in any session. If any version of an object is used by another object, the query returns the most recent version of the object. This occurs even when the most recent version of the object is unused. The query does not return workflows or cubes because these objects cannot be used by other objects.	Equals	Unused, Used
ShortcutStatus	Displays objects based on shortcut status. If you select this option, the query returns local and global shortcut objects. Shortcut objects are considered valid regardless of whether the objects they reference are valid.	Equals	Is Not Shortcut, Is Shortcut
Reusable Status	Displays reusable or non-reusable objects.	Equals, In	Non-reusable, Reusable
User	Displays objects checked in or checked out by the specified user.	Equals, In, Not Equals, Not In	Users in specified repository
ValidStatus	Displays valid or invalid objects. The Repository Service validates an object when you run validation or save an object to the repository.	Equals	Invalid, Valid
VersionStatus	Displays objects based on deleted or non-deleted status. You can specify this parameter for versioned repositories only.	Equals, In	Deleted, Not deleted

## Delete

Löscht die Repository-Tabellen aus der Repository-Datenbank.

Bevor Sie den Delete-Befehl verwenden können, müssen Sie eine Verbindung zum Repository herstellen und einen Benutzernamen und ein Passwort oder eine Passwort-Umgebungsvariable eingeben.

Wenn Sie den Delete-Befehl verwenden, muss der Repository Service im exklusiven Modus ausgeführt werden. Sie können die Ausführung des Repository Service im exklusiven Modus im Administrator-Tool konfigurieren oder den Befehl *infacmd* UpdateRepositoryService verwenden.

Der Delete-Befehl verwendet die folgende Syntax:

```
delete

[-x <repository_password_for_confirmation> |

-X <repository_password_environment_variable_for_confirmation>]

[-f (forceful delete: unregisters local repositories and deletes)]
```

In der folgenden Tabelle werden die *pmrep* Delete-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-x	repository_password_for_confirmation	Optional. Passwort. Sie können die Option -x oder -X Option verwenden, aber nicht beide. Wenn Sie weder die Option -x noch -X verwenden, werden Sie von <i>pmrep</i> aufgefordert, zur Bestätigung das Passwort einzugeben.
-X	repository_password_environment_variable_for_confirmation	Optional. Passwort-Umgebungsvariable. Sie können die Option -x oder -X Option verwenden, aber nicht beide. Wenn Sie weder die Option -x noch -X verwenden, werden Sie von <i>pmrep</i> aufgefordert, zur Bestätigung das Passwort einzugeben.
-f	-	Optional. Löscht ein globales Repository und hebt die Registrierung lokaler Repositories auf. Alle registrierten lokalen Repositories müssen ausgeführt werden.

## DeleteConnection

Löscht eine relationale Verbindung aus dem Repository.

Der DeleteConnection-Befehl verwendet die folgende Syntax:

```
deleteconnection

-n <connection_name>

[-f (force delete)]

[-s <connection type application, relational, ftp, loader or queue>]
```

In der folgenden Tabelle werden die *pmrep* DeleteConnection-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-n	connection_name	Erforderlich. Name der zu löschenden Verbindung.
-f	-	Optional. Verbindung wird ohne weitere Bestätigung gelöscht.
-s	Verbindungstypanwendung, relational, FTP, Loader oder Warteschlange	Optional. Typ der Verbindung. Folgende Verbindungstypen sind möglich: <ul style="list-style-type: none"><li>- Anwendung</li><li>- FTP</li><li>- Loader</li><li>- Warteschlange</li><li>- Relational</li></ul> Standardwert ist relational.

## DeleteDeploymentGroup

Löscht eine Bereitstellungsgruppe. Wenn Sie eine statische Bereitstellungsgruppe löschen, entfernen Sie auch alle Objekte aus der Bereitstellungsgruppe.

Der DeleteDeploymentGroup-Befehl verwendet die folgende Syntax:

```
deletedeploymentgroup  
-p <deployment_group_name>  
[-f (force delete)]
```

In der folgenden Tabelle werden die *pmrep* DeleteDeploymentGroup-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-p	deployment_group_name	Erforderlich. Name der zu löschenden Bereitstellungsgruppe.
-f	-	Optional. Löscht die Bereitstellungsgruppe ohne Bestätigung. Wenn Sie dieses Argument auslassen, werden Sie von <i>pmrep</i> vor dem Löschen der Bereitstellungsgruppe aufgefordert, dies zu bestätigen.

## DeleteFolder

Löscht einen Ordner aus dem Repository.

Der DeleteFolder-Befehl verwendet die folgende Syntax:

```
deletefolder  
-n <folder_name>
```

In der folgenden Tabelle werden die *pmrep* DeleteFolder-Option und das Argument beschrieben:

Option	Argument	Beschreibung
-n	folder_name	Erforderlich. Name des Ordners.

## DeleteLabel

Löscht eine Beschriftung und entfernt die Beschriftung aus allen Objekte, die sie verwenden. Wenn die Beschriftung gesperrt ist, schlägt das Löschen fehl.

Der DeleteLabel-Befehl verwendet die folgende Syntax:

```
deletelabel  
  
-a <label_name>  
  
[-f (force delete)]
```

In der folgenden Tabelle werden die *pmrep* DeleteLabel-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-a	label_name	Erforderlich. Name der zu löschenden Beschriftung.
-f	-	Optional. Löschen der Beschriftung ohne Bestätigung. Wenn Sie dieses Argument auslassen, werden Sie durch den Befehl aufgefordert, das Löschen der Beschriftung zu bestätigen.

## DeleteObject

Löscht ein Objekt. Verwenden Sie DeleteObject zum Löschen von Quellen, Targets, benutzerdefinierten Funktionen, Mapplets, Mappings, Sitzungen, Worklets oder Arbeitsabläufen.

Der DeleteObject-Befehl verwendet die folgende Syntax:

```
DeleteObject  
  
-o <object_type>  
  
-f <folder_name>  
  
-n <object_name>  
  
[-s dbd_separator]
```

In der folgende Tabelle werden die *pmrep* DeleteObject-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	object_type	Erforderlich. Typ des Objekts, das Sie löschen: Quelle, Target, Mapplet, Mapping, Sitzung, "benutzerdefinierte Funktion", Worklet, Arbeitsablauf.
-f	folder_name	Erforderlich. Name des Ordners, der das Objekt enthält.
-n	object_name	Erforderlich. Name des zu löschenden Objekts. Wenn Sie eine Quellddefinition löschen, müssen Sie den Datenbanknamen voranstellen. Beispiel: DBD.sourcename.
-s	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name\source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.

**Hinweis:** Sie können den DeleteObject-Befehl bei einem nicht versionsgesteuerten Repository ausführen. Wenn Sie den DeleteObject-Befehl bei einem versionsgesteuerten Repository ausführen, gibt *pmrep* den folgenden Fehler zurück:

```
This command is not supported because the versioning is on for the repository
<Repository name>.
Failed to execute DeleteObject
```

## DeleteQuery

Löscht eine Objektabfrage aus dem Repository. Sie können eine Objektabfrage, die einer Bereitstellungsgruppe zugeordnet ist, nicht löschen.

Der Befehl „DeleteQuery“ verwendet die folgende Syntax:

```
deletequery
-n <query_name>
-t <query_type (shared or personal)>
[-f (force delete)]
```

In der folgenden Tabelle werden die Optionen und Argumente für „*pmrep* DeleteQuery“ beschrieben:

Option	Argument	Beschreibung
-n	query_name	Erforderlich. Name der zu löschenden Abfrage.
-t	query_type	Erforderlich. Der Typ der Abfrage. Sie können die gemeinsame oder persönliche Nutzung festlegen.
-f	-	Optional. Löschen Sie die Abfrage ohne Bestätigung. Wenn Sie dieses Argument auslassen, werden Sie aufgefordert, das Löschen der Abfrage zu bestätigen.



# DeployDeploymentGroup

Stellt eine Bereitstellungsgruppe bereit. Sie können mit diesem Befehl eine Bereitstellungsgruppe innerhalb eines Repositorys oder in ein anderes Repository kopieren.

Zum Verwenden dieses Befehls müssen Sie eine Steuerdatei mit allen Spezifikationen erstellen, die der Assistent zum Kopieren benötigt. Die Steuerdatei ist eine XML-Datei, die von der Datei `depcntl.dtd` definiert ist.

Wenn *pmrep* nicht sofort Objektsperren im Target-Repository abrufen kann, wartet er standardmäßig unbegrenzt darauf, die Sperren abzurufen.

Sie können mit den Bereitstellungs-Steuerdatei-Parametern ein Bereitstellungs-Timeout festlegen. Das Bereitstellungs-Timeout ist der Zeitraum (in Sekunden), den *pmrep* auf das Abrufen von Sperren wartet. Bei dem Wert 0 schlägt die Bereitstellung fehl, wenn *pmrep* nicht sofort Sperren abrufen kann. Der Standardwert ist -1, wodurch *pmrep* angewiesen wird, unbegrenzt auf das Abrufen von Sperren zu warten.

Drücken Sie während des Bereitstellungsvorgangs oder während *pmrep* auf das Abrufen von Objektsperren wartet die Tastenkombination Strg+C, um die Bereitstellung abzubrechen.

Der BereitstellungsGruppeBereitstellen-Befehl verwendet die folgende Syntax:

```
deploydeploymentgroup
-p <deployment_group_name>
-c <control_file_name>
-r <target_repository_name>
[-n <target_repository_user_name>
[-s <target_repository_user_security_domain>
[-x <target_repository_password> |
-X <target_repository_password_environment_variable>]
[-d <target_domain_name> |
{-h <target_portal_host_name>
-o <target_portal_port_number>}}] (only if target is in a different domain)
[-l <log_file_name>]
```

In der folgenden Tabelle werden die *pmrep* BereitstellungsGruppeBereitstellen-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-p	deployment_group_name	Erforderlich. Name der bereitzustellenden Gruppe.
-c	control_file_name	Erforderlich. Name der XML-Datei, die die Spezifikationen des Assistenten zum Kopieren enthält. Die Bereitstellungs-Steuerdatei ist erforderlich.
-r	target_repository_name	Erforderlich. Name des Target-Repositorys, in dem Sie die Bereitstellungsgruppe kopieren.

Option	Argument	Beschreibung
-n	target_repository_user_name	Erforderlich, wenn Sie die Bereitstellungsgruppe in ein anderes Repository kopieren. Anmeldebenutzername für das Target-Repository.
-s	target_repository_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Die Standardeinstellung ist "Native".
-x	target_repository_password	Optional. Anmelde-Passwort für das Target-Repository. Verwenden Sie die Option -x oder -X, aber nicht beide. Wenn Sie die Bereitstellungsgruppe in ein anderes Repository kopieren und keine der beiden Optionen -x oder -X verwenden, werden Sie von <i>pmrep</i> zur Eingabe des Passworts aufgefordert.
-X	target_repository_password_environment_variable	Optional. Anmelde-Passwort-Umgebungsvariable für das Target-Repository. Verwenden Sie die Option -x oder -X, aber nicht beide. Wenn Sie die Bereitstellungsgruppe in ein anderes Repository kopieren und keine der beiden Optionen -x oder -X verwenden, werden Sie von <i>pmrep</i> zur Eingabe des Passworts aufgefordert.
-d	target_domain_name	Erforderlich, wenn Sie die Bereitstellungsgruppe in ein anderes Repository kopieren, ohne die Optionen -h und -o zu verwenden. Name der Domäne für das Repository.
-h	target_portal_host_name	Erforderlich, wenn Sie die Bereitstellungsgruppe in ein anderes Repository kopieren, ohne die Option -d zu verwenden. Name des Computers für den Knoten, der als Host für die Domäne des Target-Repositorys eingesetzt wird.
-o	target_portal_port_number	Erforderlich, wenn Sie die Bereitstellungsgruppe in ein anderes Repository kopieren, ohne die Option -d zu verwenden. Portnummer für den Knoten, der als Host für die Domäne des Target-Repositorys eingesetzt wird.
-l	log_file_name	Optional. Protokolldatei, die die einzelnen Bereitstellungsschritte aufzeichnet. Wenn Sie diese Option auslassen, gibt <i>pmrep</i> die Bereitstellungsschritte im Befehlszeilenfenster aus.

## DeployFolder

Stellen einen Ordner bereit. Sie können mit diesem Befehl einen Ordner innerhalb eines Repositorys oder in ein anderes Repository kopieren.

Zum Verwenden dieses Befehls müssen Sie eine Steuerdatei mit allen Spezifikationen erstellen, die der Assistent zum Kopieren benötigt. Die Steuerdatei ist eine XML-Datei, die von der Datei `depcntl.dtd` definiert ist.

Wenn *pmrep* nicht sofort Objektsperren im Target-Repository abrufen kann, wartet er standardmäßig unbegrenzt darauf, die Sperren abzurufen.

Sie können mit den Bereitstellungs-Steuerdatei-Parametern ein Bereitstellungs-Timeout festlegen. Das Bereitstellungs-Timeout ist der Zeitraum (in Sekunden), den *pmrep* auf das Abrufen von Sperren wartet. Bei

dem Wert 0 schlägt die Bereitstellung fehl, wenn *pmrep* nicht sofort Sperren abrufen kann. Der Standardwert ist -1, wodurch *pmrep* angewiesen wird, unbegrenzt auf das Abrufen von Sperren zu warten.

Drücken Sie während des Bereitstellungsvorgangs oder während *pmrep* auf das Abrufen von Objektsperren wartet die Tastenkombination Strg+C, um die Bereitstellung abzubrechen.

Der DeployFolder-Befehl verwendet die folgende Syntax:

```
deployfolder
-f <folder_name>
-c <control_file_name>
-r <target_repository_name>
[-n <target_repository_user_name>
[-s <target_repository_user_security_domain>]
[-x <target_repository_password> |
-X <target_repository_password_environment_variable>]
[-d <target_domain_name> |
{-h <target_portal_host_name>
-o <target_portal_port_number>}}] (only if target is in a different domain)
[-l <log_file_name>]
```

In der folgenden Tabelle werden die *pmrep* DeployFolder-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-f	folder_name	Erforderlich. Name des bereitzustellenden Ordners.
-c	control_file_name	Erforderlich. Name der XML-Datei, die die Spezifikationen des Assistenten zum Kopieren enthält.
-r	target_repository_name	Erforderlich. Name des Target-Repositorys, in das Sie den Ordner kopieren.
-n	target_repository_user_name	Erforderlich, wenn Sie den Ordner in ein anderes Repository kopieren. Anmeldebenutzername für das Target-Repository.
-s	target_repository_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Die Standardeinstellung ist "Native".
-x	target_repository_user_password	Optional. Anmelde-Passwort für das Target-Repository. Verwenden Sie die Option -x oder -X, aber nicht beide. Wenn Sie den Ordner in ein anderes Repository kopieren und keine der beiden Optionen -x oder -X verwenden, werden Sie von <i>pmrep</i> zur Eingabe des Passworts aufgefordert.
-X	target_repository_password_environment_variable	Optional. Anmelde-Passwort-Umgebungsvariable für das Target-Repository. Verwenden Sie die Option -x oder -X, aber nicht beide. Wenn Sie den Ordner in ein anderes Repository kopieren und keine der beiden Optionen -x oder -X verwenden, werden Sie von <i>pmrep</i> zur Eingabe des Passworts aufgefordert.

Option	Argument	Beschreibung
-d	target_domain_name	Erforderlich, wenn Sie den Ordner in ein anderes Repository kopieren, ohne die Optionen -h und -o zu verwenden. Name der Domäne für das Repository.
-h	target_portal_host_name	Erforderlich, wenn Sie den Ordner in ein anderes Repository kopieren, ohne die Option -d zu verwenden. Name des Computers für den Knoten, der als Host für die Domäne des Target-Repositorys eingesetzt wird.
-o	target_portal_port_number	Erforderlich, wenn Sie den Ordner in ein anderes Repository kopieren, ohne die Option -d zu verwenden. Portnummer für den Knoten, der als Host für die Domäne des Target-Repositorys eingesetzt wird.
-l	log_file_name	Optional. Protokolldatei, die die einzelnen Bereitstellungsschritte aufzeichnet. Wenn Sie diese Option auslassen, gibt <i>pmrep</i> die Bereitstellungsschritte im Befehlszeilenfenster aus.

## ExecuteQuery

Führt eine Abfrage aus. Sie können angeben, ob das Ergebnis angezeigt oder in eine persistente Eingabedatei geschrieben werden soll. Wenn die Abfrage erfolgreich ist, wird die Gesamtanzahl der qualifizierten Datensätze geliefert.

Verwenden Sie die persistente Eingabedatei mit den Befehlen ApplyLabel, AddToDeploymentGroup, MassUpdate und Validate.

Der ExecuteQuery-Befehl verwendet die folgende Syntax:

```
executequery
-q <query_name>
[-t <query_type (shared or personal)>]
[-u <output_persistent_file_name>]
[-a (append)]
[-c <column_separator>]
[-r <end-of-record_separator>]
[-l <end-of-listing_indicator>]
[-b (verbose)]
[-y (print database type)]
[-n (do not include parent path)]
[-s <dbd_separator>]
```

In der folgenden Tabelle werden die *pmrep* ExecuteQuery-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-q	query_name	Erforderlich. Name der auszuführenden Abfrage.
-t	query_type	Optional. Typ der auszuführenden Abfrage. Sie können festlegen, ob es sich um öffentliche oder private Abfragen handelt. Wenn nicht anders angegeben, sucht <i>pmrep</i> zuerst in allen privaten Abfragen nach dem entsprechenden Abfragenamen. Danach werden die öffentlichen Abfragen durchsucht.
-u	persistent_output_file_name	Optional. Senden Sie das Abfrageergebnis in eine Textdatei. Wenn Sie keinen Dateinamen eingeben, wird das Abfrageergebnis in "stdout" ausgegeben.
-a	-	Optional. Hängt die Abfrageergebnisse an die persistente Ausgabedatei an. Wenn Sie diese Option nicht eingeben, überschreibt <i>pmrep</i> den Inhalt der Datei.
-c	column_separator	Optional. Zeichen oder Zeichenfolgen, mit denen Spalten mit Objektmetadaten getrennt werden. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Wenn ein Repository-Objektname Leerzeichen enthält, sollten Sie kein Leerzeichen als Spaltentrenner verwenden. Wenn Sie diese Option auslassen, verwendet <i>pmrep</i> ein einzelnes Leerzeichen.
-r	end-of-record_separator	Optional. Zeichen oder Zeichenfolgen, die das Ende von Objektmetadaten kennzeichnen. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Wenn Sie diese Option auslassen, verwendet <i>pmrep</i> eine neue Zeile.
-l	end-of-listing_indicator	Optional. Zeichen oder Zeichenfolgen, die das Ende der Objektliste kennzeichnen. Geben Sie ein Zeichen oder eine Zeichenfolge ein, die nicht in Repository-Objektnamen verwendet wird. Wenn Sie diese Option auslassen, verwendet <i>pmrep</i> einen Punkt.
-b	-	Optional. Verbose. Zeigt neben den Mindestinformationen weitere Informationen zu den Objekten an. Wenn Sie diese Option auslassen, druckt <i>pmrep</i> ein reduziertes Format, einschließlich Objekttyp, wiederverwendbare oder nicht wiederverwendbare Wörter, Objektname und -pfad. Verbose-Format enthält den Objektstatus, die Versionsnummer, den Ordernamen und ausgecheckte Informationen. Das Kurzformat für globale Objekte, z. B. Beschriftung, Abfrage, Bereitstellungsgruppe und Verbindung, enthält den Objekttyp und den Objektnamen. Verbose-Format enthält den Beschriftungstyp, den Abfragetyp, den Bereitstellungsgruppen-Typ, den Erstellernamen sowie den Zeitpunkt der Erstellung.
-y	-	Optional. Zeigt den Datenbanktyp von Quellen und Zielen an.

Option	Argument	Beschreibung
-n	-	Optional. Schließt im Abfrageergebnis nicht den vollständigen übergeordneten Pfad der nicht wiederverwendbaren Objekte ein. Wenn Sie beispielsweise diese Option verwenden und das Ergebnis enthält eine nicht wiederverwendbare Transformation, druckt <i>pmrep</i> <i>transformation_name</i> statt <i>mapping_name.transformation_name</i> . Diese Option kann die Leistung von <i>pmrep</i> erhöhen.
-s	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt <i>database_name.source_name</i> das Quellobjekt als <i>database_name \source_name</i> , und legen Sie als <i>dbd_separator</i> den umgekehrten Schrägstrich (\) fest.

## Exit

Beendet den interaktiven Modus von *pmrep*.

Bei jeder Befehlseingabe wird *pmrep* vom Befehlszeilenmodus aufgerufen und beendet.

Der Exit-Befehl verwendet die folgende Syntax:

```
exit
```

## FindCheckout

Zeigt eine Liste der ausgecheckten Objekte im Repository an. Die Auflistung enthält die ausgecheckten Einträge, außer wenn Sie "alle Benutzer" eingeben.

Wenn Sie einen Objekttyp auswählen, können Sie ausgecheckte Objekte in einem bestimmten Ordner oder in allen Ordnern auflisten. Wenn Sie keinen Objekttyp angeben, gibt *pmrep* alle ausgecheckten Objekte im Repository zurück.

Der FindCheckout-Befehl verwendet die folgende Syntax:

```
findcheckout
[-o <object_type>]
[-f <folder_name>]
[-u (all_users)]
[-c <column_separator>]
[-r <end-of-record_separator>]
[-l <end-of-listing_indicator>]
[-b (verbose)]
[-y (print database type)]
```

`[-s <dbd_separator>]`

In der folgenden Tabelle werden die *pmrep* FindCheckout-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	object_type	Aufzulistender Objekttyp. Sie können Quelle, Ziel, Umwandlung, Mapping, Sitzung, Worklet, Arbeitsablauf, Scheduler, Sitzungskonfiguration, Aufgabe, Cube oder Größenordnung festlegen. Wenn Sie diese Option nicht verwenden, ignoriert <i>pmrep</i> die Optionen -f und -u und der Befehl gibt alle ausgecheckten Objekte im Repository zurück.
-f	folder_name	Optional, wenn Sie einen Objekttyp angeben. Gibt eine Liste der ausgecheckten Objekte für den Objekttyp im angegebenen Ordner zurück. Standardmäßig werden Objekte für den Objekttyp ordnerübergreifend aufgelistet.
-u	-	Optional. Listen Sie die ausgecheckten Objekte aller Benutzer auf. Standardmäßig werden ausgecheckte Objekte des aktuellen Benutzers aufgelistet.
-c	column_separator	Optional. Zeichen oder Zeichenfolgen, mit denen Spalten mit Objektmetadaten getrennt werden.  Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Wenn ein Repository-Objektnamen Leerzeichen enthält, sollten Sie kein Leerzeichen als Spaltentrenner verwenden.  Wenn Sie diese Option auslassen, verwendet <i>pmrep</i> ein einzelnes Leerzeichen.
-r	end-of-record_separator	Optional. Zeichen oder Zeichenfolgen, die das Ende von Objektmetadaten kennzeichnen. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Standardmäßig wird für eine neue Zeile /n verwendet.
-l	end-of-listing_indicator	Optional. Zeichen oder Zeichenfolgen, die das Ende der Objektliste kennzeichnen. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Wenn Sie diese Option auslassen, verwendet <i>pmrep</i> einen Punkt.
-b	-	Optional. Verbose. Zeigt neben den Mindestinformationen weitere Informationen zu den Objekten an. Wenn Sie diese Option auslassen, druckt <i>pmrep</i> ein reduziertes Format, einschließlich Objekttyp, wiederverwendbare oder nicht wiederverwendbare Wörter, Objektname und -pfad. Verbose-Format enthält die Versionsnummer und den Ordernamen.  Das Kurzformat für globale Objekte wie Beschriftung, Abfrage, Bereitstellungsgruppe und Verbindung enthält den Objekttyp und den Objektnamen. Verbose-Format enthält den Erstellernamen und den Zeitpunkt der Erstellung.

Option	Argument	Beschreibung
-y	-	Optional. Zeigt den Datenbanktyp von Quellen und Zielen an.
-s	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name \source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.

## GetConnectionDetails

Listet die Eigenschaften und Attribute eines Verbindungsobjekts als Name-Wert-Paar auf.

Für die Verwendung des GetConnectionDetails-Befehls benötigen Sie die Leseberechtigung für das Verbindungsobjekt.

Der GetConnectionDetails-Befehl verwendet die folgende Syntax:

```
getconnectiondetails
-n <connection_name>
-t <connection_type>
```

In der folgenden Tabelle werden die *pmrep* GetConnectionDetails-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-n	connection_name	Erforderlich. Name der Verbindung, für die Details aufgelistet werden sollen.
-t	connection_type	Erforderlich. Typ der Verbindung. Folgende Verbindungstypen sind möglich: <ul style="list-style-type: none"> <li>- Application</li> <li>- FTP</li> <li>- Loader</li> <li>- Warteschlange</li> <li>- Relational</li> </ul>

## GenerateAbapProgramToFile

Generiert das ABAP-Programm für ein Mapping mit SAP-Tabelle als Quelle und speichert das Programm als Datei. Der GenerateAbapProgramToFile-Befehl generiert das ABAP-Programm für ein Mapping im PowerCenter Repository. Das generierte Programm wird als Datei gespeichert. Sie können den GenerateAbapProgramToFile-Befehl für Mappings verwenden, die als Quelle SAP-Tabellen benutzen.

Die Benennungskonvention für die Datei lautet *mappingname\_<version>\_<program\_mode>.ab4*. Sie müssen den Pfad und den Dateinamen in doppelte Anführungszeichen einschließen. Nachdem Sie das ABAP-



Programm generiert und in eine Datei gespeichert haben, verwenden Sie den InstallAbapProgram-Befehl, um es auf einem SAP-System zu installieren.

Der GenerateAbapProgramToFile-Befehl verwendet die folgende Syntax:

```
generateabaprogramtofile
-s <folder_name>
-m <mapping_name>
[-v <version_number>]
[-l <log_filename>]
-u <user_name>
-x <password>
-c <connect_string>
-t <client>
[-y <language>]
-p <program_mode (file, stream)>
-f <output_file_location>
{-e (enable override)
-o <override_name> }
[-a (authority check)]
[-n (use namespace)]
```

In der folgenden Tabelle werden die pmrep GenerateAbapProgramToFile-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-s	folder_name	Erforderlich. Der Name des Ordners, der das Mapping enthält, für das das ABAP-Programm generiert werden muss.
-m	mapping_name	Erforderlich. Name des Mappings.
-v	version_number	Optional. Versionsnummer des Mappings. Standardmäßig ist die neueste Version.
-l	log_filename	Optional. Name der Protokolldatei, in die die Informationen oder Fehlermeldungen geschrieben werden. Standardmäßig wird die Protokolldatei in dem Verzeichnis erstellt, in dem Sie den Befehl ausführen.
-u	user_name	Erforderlich. Benutzername für die SAP-Quellsystemverbindung. Muss ein Benutzer sein, für den Sie eine Quellsystemverbindung erstellt haben.
-x	passwort	Erforderlich. Passwort für den Benutzernamen. Verwenden Sie das Befehlszeilenprogramm pmpasswd zum Verschlüsseln des Benutzerpassworts.
-c	connect_string	Erforderlich. In der Datei <code>sapnwrfc.ini</code> definierter DEST-Eintrag für eine Verbindung mit einem bestimmten SAP-Anwendungsserver oder für eine Verbindung, die den SAP-Lastenausgleich verwendet.

Option	Argument	Beschreibung
-t	Client	Erforderlich. SAP-Clientnummer.
-y	Sprache	Optional. SAP-Anmeldesprache. Muss mit der Codepage des PowerCenter Client kompatibel sein. Standardwert ist die Sprache des SAP-Systems.
-p	program_mode (file, stream)	Erforderlich. Modus, in denen der PowerCenter-Integrationsdienst Daten aus dem SAP-System extrahiert. Wählen Sie die Datei oder den Stream aus.
-f	output_file_location	Erforderlich. Speicherort im lokalen Rechner, auf dem Sie die ABAP-Programmdatei speichern möchten.
-e	-	Optional. Überschreibt den standardmäßigen Namen der ABAP-Programmdatei.
-o	override_name	Erforderlich, wenn Sie das Überschreiben aktivieren. ABAP-Programmdateiname.
-a	-	Optional. Fügt dem ABAP-Programm Autoritätsprüfungen hinzu.
-n	-	Optional. Hängt dem ABAP-Programmnamen einen Namespace an, den Sie bei SAP registriert haben.

## Beispiel

Im folgenden Beispiel wird ein ABAP-Programm generiert und in einer Datei gespeichert:

```
generateabaprogramtofile -s folder_name -m mapping_name -l logfile_name -u user_name -x
password -c connect_string -t 800 -y EN -p stream -e -o program_name -n -a -f
"C:\<informatica_installation_dir>\ABAP_prog"
```

## Hilfe

Gibt die Syntax für den angegebenen Befehl zurück. Wenn Sie keinen Befehl angeben, wird die Syntax für alle *pmrep*-Befehle angezeigt.

Verwenden Sie für den Help-Befehl eine der folgenden Syntaxstrukturen:

```
help [command]
-help [command]
```

## InstallAbapProgram

Installiert ein ABAP-Programm in das SAP-System. Verwenden Sie den InstallAbapProgram-Befehl, um das ABAP-Programm zu generieren und direkt auf dem SAP-System zu installieren. Sie können mit diesem Befehl ein ABAP-Programm aus einer Datei auf dem SAP-System installieren. Sie können den InstallAbapProgram-Befehl für Mappings verwenden, die SAP-Tabellen als Quelle nutzen.

Der InstallAbapProgram-Befehl ruft die Mapping-Informationen über das PowerCenter Repository für ein Mapping ab und generiert das ABAP-Programm. Der Befehl installiert das generierte ABAP-Programm in das SAP-System. Wenn Sie das ABAP-Programm zum ersten Mal auf dem SAP-System installieren, generiert der

Befehl einen Programmnamen. Nachfolgende Installationen verwenden den gleichen Programmnamen, wenn Sie den gleichen Programmmodus nutzen.

Wenn Sie ein ABAP-Programm über eine Datei auf dem SAP-System installieren, müssen Sie den vollständigen Pfad und den Dateinamen des zu installierenden ABAP-Programms zur Verfügung stellen. Schließen Sie den Pfad und den Dateinamen in doppelte Anführungszeichen ein. Sie müssen den Ordernamen und die Mapping-Informationen angeben, für die das ABAP-Programm generiert wurde. Der InstallAbapProgram-Befehl ruft die Beschreibung des Mappings ab und hängt sie an das ABAP-Programm an, wenn es auf dem SAP-System installiert wird.

Der InstallAbapProgram-Befehl verwendet die folgende Syntax:

```
installabaprogram
-s <folder_name>
-m <mapping_name>
[-v <version_number>]
[-l <log_filename>]
-u <user_name>
-x <password>
-c <connect_string>
-t <client>
[-y <language>]
{-f <input_file_name> |
-p <program_mode (file, stream)>
-e (enable override)
-o <override_name> }
[-a (authority check)]
[-n (use namespace)]
[-d <development_class_name>]
```

In der folgenden Tabelle werden die pmrep InstallAbapProgram-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-s	folder_name	Erforderlich. Der Name des Ordners, der das Mapping enthält, für das das ABAP-Programm generiert werden muss. Bei Installation über eine Datei der Name des Ordners, der das Mapping enthält, für das Sie das ABAP-Programm generiert haben.
-m	mapping_name	Erforderlich. Name des Mappings. Bei Installation über eine Datei der Name des Mappings, für das Sie das ABAP-Programm generiert haben.
-v	version_number	Optional. Versionsnummer des Mappings. Standardmäßig ist die neueste Version. Bei Installation über eine Datei die Version des Mappings, für das Sie das ABAP-Programm generiert haben.

Option	Argument	Beschreibung
-l	log_filename	Optional. Name der Protokolldatei, in die die Informationen oder Fehlermeldungen geschrieben werden. Standardmäßig wird die Protokolldatei in dem Verzeichnis gespeichert, in dem Sie den Befehl ausführen.
-u	user_name	Erforderlich. Benutzername für die SAP-Quellsystemverbindung. Muss ein Benutzer sein, für den Sie eine Quellsystemverbindung erstellt haben.
-x	passwort	Erforderlich. Passwort für den Benutzernamen. Verwenden Sie das Befehlszeilenprogramm pmpasswd zum Verschlüsseln des Benutzerpassworts.
-c	connect_string	Erforderlich. In der Datei <code>sapnwrfc.ini</code> definierter DEST-Eintrag für eine Verbindung mit einem bestimmten SAP-Anwendungsserver oder für eine Verbindung, die den SAP-Lastenausgleich verwendet.
-t	Client	Erforderlich. SAP-Clientnummer.
-y	Sprache	Optional. SAP-Anmeldesprache. Muss mit der Codepage des PowerCenter Client kompatibel sein. Standardwert ist die Sprache des SAP-Systems.
-f	input_file_name	Erforderlich, wenn Sie das ABAP-Programm mit einer Datei installieren. Name der ABAP-Programmdatei, von der aus Sie das ABAP-Programm in das SAP-System installieren möchten.
-p	program_mode (file, stream)	Erforderlich, wenn Sie das ABAP-Programm direkt auf dem SAP-System generieren und installieren. Optional, wenn Sie das ABAP-Programm mit einer Datei installieren. Modus, in denen der PowerCenter-Integrationsdienst Daten aus dem SAP-System extrahiert. Wählen Sie die Datei oder den Stream aus.
-e	-	Optional, wenn Sie das ABAP-Programm direkt auf dem SAP-System generieren und installieren. Überschreibt den standardmäßigen Namen der ABAP-Programmdatei.
-o	override_name	Erforderlich, wenn Sie das Überschreiben aktivieren. ABAP-Programmdateiname.
-a	-	Optional, wenn Sie das ABAP-Programm direkt auf dem SAP-System generieren und installieren. Fügt dem ABAP-Programm Autoritätsprüfungen hinzu.
-n	-	Optional, wenn Sie das ABAP-Programm direkt auf dem SAP-System generieren und installieren. Hängt dem ABAP-Programmnamen einen Namespace an, den Sie bei SAP registriert haben.
-d	development_class_name	Optional. Paket oder der Name der Entwicklungsklasse, in der der PowerCenter-Repository-Dienst das ABAP-Programm installiert. Standardentwicklungsklasse ist \$TMP.

## Beispiele

Das folgende Beispiel installiert das ABAP-Programm direkt auf dem SAP-System:

```
installabaprogram -s folder_name -m mapping_name -l logfile_name -u user_name -x
password -c connect_string -t 800 -y EN -p file -e -o zabc -a -n -d development_class
```

Das folgende Beispiel installiert das ABAP-Programm von einer Datei auf dem SAP-System:

```
installabaprogram -s folder_name -m mapping_name -l logfile_name -u user_name -x
password -c connect_string -t 800 -y EN -p file -v 1 -f
"C:\mapping_name_version_file.ab4"
```

# KillUserConnection

Beendet Benutzerverbindungen zum Repository. Sie können Benutzerverbindungen basierend auf dem Benutzernamen oder der Verbindungs-ID beenden. Sie können auch alle Benutzerverbindungen zum Repository beenden.

Der KillUserConnection-Befehl verwendet die folgende Syntax:

```
killuserconnection
{-i <connection_id> |
-n <user_name> |
-a (kill all)}
```

In der folgenden Tabelle werden die *pmrep* KillUserConnection-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-i	connection_id	Repository-Verbindungs-ID.
-n	user_name	Benutzername.
-a	-	Beendet alle Verbindungen.

# ListConnections

Listet alle Verbindungsobjekte im Repository und deren jeweilige Verbindungstypen auf. Folgende Verbindungstypen sind möglich:

- Anwendung
- FTP
- Loader
- Warteschlange
- Relational

Der ListConnections-Befehl verwendet die folgende Syntax:

```
listconnections
[-t (output includes connection subtype)]
```

In der folgenden Tabelle wird die *pmrep* ListConnections-Option beschrieben:

Option	Argument	Beschreibung
-t	-	Optional. Zeigt den Verbindungsuntertyp an. Bei einer relationalen Verbindung gehören zu den Verbindungsuntertypen beispielsweise Oracle, Sybase und Microsoft SQL Server. Sie können den Untertyp nur für Verbindungen anzeigen, für die Sie eine Leseberechtigung haben.

Weitere Informationen über Verbindungsuntertypen finden Sie unter ["Verbindungsuntertypen" auf Seite 1445](#).

# ListObjectDependencies

Lists dependency objects for reusable and non-reusable objects. If you want to list dependencies for non-reusable objects, you must use a persistent input file containing object IDs. You can create this file by running a query and choosing to create a text file.

ListObjectDependencies accepts a persistent input file and it can create a persistent output file. These files are the same format. If you create an output file, use it as input to the ApplyLabel, AddToDeployment Group, or Validate *pmrep* commands.

ListObjectDependencies returns the number of records if the command runs successfully.

The ListObjectDependencies command uses the following syntax:

```
listobjectdependencies
{{-n <object_name>
  -o <object_type>
  [-t <object_subtype>]
  [-v <version_number>]
  [-f <folder_name>] } |
  -i <persistent_input_file>}
[-d <dependency_object_types>]
[-p <dependency_direction (children, parents, or both)>]
[-s (include pk-fk dependency)]
[-g (across repositories)]
[-u <persistent_output_file_name>
  [-a (append)]]
[-c <column_separator>]
[-r <end-of-record_separator>]
[-l <end-of-listing_indicator>]
[-b (verbose)]
[-y (print database type)]
[-e <dbd_separator>]
```

The following table describes *pmrep* ListObjectDependencies options and arguments:

Option	Argument	Description
-n	object_name	Required. Name of a specific object to list dependencies for.
-o	object_type	Required. Object type to list dependencies for. You can specify source, target, transformation, mapping, session, worklet, workflow, scheduler, session, session config, task, cube, dimension, query and deploymentgroup.

Option	Argument	Description
-t	object_subtype	Type of transformation, task, or query. Ignored for other object types. For more information about valid subtypes, see <a href="#">“Listing Object Types” auf Seite 1494</a> .
-v	version_number	Optional. List dependent objects for an object version other than the latest version. You must use this option only for versioned repositories. It does not apply to non-versioned repositories.
-f	folder_name	Folder containing object name. Folder is required if you do not use the -i option.
-i	persistent_input_file	Optional. Text file of objects generated from ExecuteQuery or Validate commands. You must use this file if you want to list dependencies for non-reusable objects. If you use this option, then you cannot use the -n, -o, -f options to specify objects.
-d	dependency_object_types	Optional. Type of dependent objects to list. You can enter ALL or one or more object types. Default is ALL. If ALL, then <i>pmrep</i> lists all supported dependent objects. If you choose one or more objects, then <i>pmrep</i> lists dependent objects for these types. To enter multiple object types, separate them by commas without spaces.
-p	dependency_direction	Required if you do not use the -s option. Parents or children dependent objects to list. You can specify parents, children, or both. If you do not use the -p option, <i>pmrep</i> does not list parent or child dependencies.
-s	-	Required if you do not use the -p option. Include the primary key-foreign key dependency object regardless of the direction of the dependency. If you do not use the -s option, <i>pmrep</i> does not list primary-key/foreign-key dependencies.
-g	-	Optional. Find object dependencies across repositories.
-u	persistent_output_file_name	Send the dependency result to a text file. Use the text file as input to the ApplyLabel, AddToDeployment Group, or Validate <i>pmrep</i> commands. The default sends the query result to stdout. You cannot use the -b and -c options with this option.
-a	-	Append the result to the persistent output file instead of overwriting it.
-c	column_separator	Character or set of characters used to separate object metadata columns. Use a character or set of characters that is not used in repository object names. If any repository object name contains spaces, you might want to avoid using a space as a column separator. You cannot use this option with the -u option. If you omit this option, <i>pmrep</i> uses a single space.
-r	end-of-record_separator	Character or set of characters used to specify the end of the object metadata. Use a character or set of characters that is not used in repository object names. Default is newline /n.

Option	Argument	Description
-l	end-of-listing_indicator	Character or set of characters used to specify the end of the object list. Enter a character or set of characters that is not used in repository object names. If you omit this option, <i>pmrep</i> uses a period.
-b	-	Verbose. Displays more than the minimum information about the objects. If you omit this option, <i>pmrep</i> displays a shorter format including the object type, the word reusable or non-reusable, the object name and path. Verbose format includes the version number and folder name. The short format for global objects, such as label, query, deployment group, and connection, includes the object type and object name. Verbose format includes the creator name and creation time. You cannot use this option with the -u option.
-y	-	Optional. Displays the database type of sources and targets.
-e	dbd_separator	Optional. If an ODBC source has a period (.) in the name, define a different separator character when you define the source object. For example, instead of database_name.source_name, define the source object as database_name\source_name, and define the dbd_separator as backslash (\).

## ListObjects

Gibt eine Liste von Objekten im Repository zurück. Wenn Sie Objekte auflisten, gibt *pmrep* Objektmetadaten zurück. Verwenden Sie die folgenden Auflistungsoperationen:

- **Auflisten von Objekttypen.** Definieren Sie die aufzulistenden Objekte.
- **Auflisten von Ordnern.** Listen Sie alle Ordner im Repository auf.
- **Auflisten von Objekten.** Listen Sie wiederverwendbare und nicht wiederverwendbare Objekte im Repository oder in einem Ordner auf.

Verwenden Sie ListObjects in einem Shell-Skript, um Objektmetadaten zurückzugeben und Metadaten zu parsen. Verwenden Sie anschließend die geparsen Daten in einem anderen *pmrep*-Befehl.

Verwenden Sie zum Beispiel ListObjects, um alle Sequenzgenerator-Transformationen im Repository aufzulisten. Erstellen Sie ein Shell-Skript, das ListObjects verwendet, um die Informationen der Sequenzgenerator-Transformation zurückzugeben, parsen Sie die von ListObjects zurückgegebenen Daten und verwenden Sie UpdateSeqGenVals, um die Sequenzwerte zu aktualisieren.

*pmrep* gibt jedes Objekt in einem Datensatz und gibt die Metadaten für jedes einzelne Objekt in einer Spalte zurück. Die Datensätze werden standardmäßig durch eine neue Zeile getrennt. Sie können die Zeichen eingeben, die zum Trennen von Datensätzen und Spalten verwendet werden. Sie können zudem die Zeichen eingeben, die das Ende einer Liste kennzeichnen.

**Tipp:** Wenn Sie Zeichen zum Trennen von Datensätzen und Spalten und zum Kennzeichnen des Listenendes eingeben, verwenden Sie Zeichen, die nicht in Repository-Objektnamen benutzt werden. Dies hilft bei der Verwendung eines Shell-Skripts zum Parsen der Objektmetadaten.



Der ListObjects-Befehl verwendet die folgende Syntax:

```
listobjects
-o <object_type>
[-t <object_subtype>]
[-f <folder_name>]
[-c <column_separator>]
[-r <end-of-record_indicator>]
[-l <end-of-listing_indicator>]
[-b (verbose)]
[-y (print database type)]
[-s <dbd_separator>]
```

In der folgenden Tabelle werden die *pmrep* ListObject-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	object_type	<p>Erforderlich. Aufzulistender Objekttyp.</p> <ul style="list-style-type: none"> <li>- Wenn Sie Ordner eingeben, muss keine andere Option eingeschlossen werden. <i>pmrep</i> ignoriert die Optionen -t und -f.</li> <li>- Wenn Sie andere Objekte als Ordner eingeben, müssen Sie die Option -f einschließen.</li> <li>- Wenn Sie Transformation oder Aufgabe eingeben, müssen Sie die Option -f einschließen. Optional können Sie die Option -t einschließen.</li> </ul> <p>Weitere Informationen über Objekttypen, die mit ListObjects verwendet werden können, finden Sie unter <a href="#">"Listing Object Types" auf Seite 1494</a>.</p>
-t	object_subtype	<p>Optional. Aufzulistender Transformations- oder Aufgabentyp. Wenn Sie Transformation oder Aufgabe als Objekttyp eingeben, können Sie diese Option einschließen, um einen bestimmten Typ zurückzugeben.</p> <p>Weitere Informationen über Objekttypen, die mit ListObjects verwendet werden können, finden Sie unter <a href="#">"Listing Object Types" auf Seite 1494</a>.</p>
-f	folder_name	<p>Erforderlich, wenn Sie andere Objekte als Ordner auflisten. Zu suchender Ordner. Verwenden Sie diese Option bei allen Objekttypen außer Bereitstellungsgruppe, Ordner, Beschriftung und Abfrage.</p>
-c	column_separator	<p>Optional. Zeichen oder Zeichenfolgen, mit denen Spalten mit Objektmetadaten getrennt werden. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Wenn ein Repository-Objektnamen Leerzeichen enthält, sollten Sie kein Leerzeichen als Spaltentrennzeichen verwenden.</p> <p>Wenn Sie diese Option auslassen, verwendet <i>pmrep</i> ein einzelnes Leerzeichen.</p>
-r	end-of-record_indicator	<p>Optional. Zeichen oder Zeichenfolgen, das bzw. die das Ende von Objektmetadaten kennzeichnen. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird.</p> <p>Standardwert ist „newline“ /n.</p>

Option	Argument	Beschreibung
-l	end_of_listing_indicator	Optional. Zeichen oder Zeichenfolgen, die das Ende der Objektliste kennzeichnen. Geben Sie ein Zeichen oder eine Zeichenfolge ein, die nicht in Repository-Objektnamen verwendet wird. Wenn Sie diese Option auslassen, verwendet <i>pmrep</i> einen Punkt.
-b	-	Optional. Verbose. Zeigen Sie neben den Mindestinformationen weitere Informationen zu den Objekten an. Wenn Sie diese Option auslassen, zeigen Sie ein reduziertes Format an, einschließlich Objekttyp, wiederverwendbare oder nicht wiederverwendbare Wörter, Objektname und -pfad. Das ausführliche Format enthält den Objektstatus, die Versionsnummer und ausgecheckte Informationen.  Das Kurzformat für globale Objekte, z. B. Beschriftung, Abfrage, Bereitstellungsgruppe und Verbindung, enthält den Objekttyp und den Objektnamen. Verbose-Format enthält den Beschriftungstyp, den Abfragetyp, den Bereitstellungsgruppen-Typ, den Erstellernamen sowie den Zeitpunkt der Erstellung.
-y	-	Optional. Zeigt den Datenbanktyp von Quellen und Zielen an.
-s	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name\source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.

## Listing Object Types

Use the `object_type` option to define the objects you want to list. The command lists the latest versions or checked out versions of objects, including shortcuts, but excluding objects according to the rules for object types.

The following table describes the object types and rules you use with `ListObjects`:

Object Type	Rule
Deploymentgroup	List deployment groups in the repository.
Folder	List folders in the repository.
Label	List labels in the repository.
Mapplet	List mapplets with latest or checked out version in a folder, including shortcuts but excluding instances of reusable mapplets.
Mapping	List mappings with latest or checked out version in a folder, including shortcuts but excluding instances of reusable mapplets.
Query	List queries in the repository.
Scheduler	List reusable and non-reusable schedulers with latest or checked out version in a folder.

Object Type	Rule
Session	List reusable and non-reusable sessions with latest or checked out version in a folder, excluding instances of reusable sessions.
Sessionconfig	List the session configurations with latest or checked out version in a folder.
Source	List sources with latest or checked out version in a folder, including shortcuts but excluding source instances.
Target	List targets with latest or checked out version in a folder, including shortcuts but excluding target instances.
Task	List reusable and non-reusable tasks with latest or checked out version in a folder.
Transformation	List reusable and non-reusable transformations with latest or checked out version in a folder, including shortcuts and excluding instances of reusable transformations.
"User Defined Function"	List user-defined functions in the repository.
Workflow	List the workflows with latest version or checked out version in a folder.
Worklet	List reusable and non-reusable worklets with latest version or checked out version in a folder, excluding instances of reusable worklets.

The following table describes the object types and values to use with *pmrep* commands:

Object Type	Subtype Value	Description
Query	personal	Personal
Query	shared	Shared
Task	assignment	Assignment
Task	command	Command
Task	control	Control
Task	decision	Decision
Task	email	Email
Task	event_raise	Event-raise
Task	event_wait	Event-wait
Task	start	Start
Task	timer	Timer
Transformation	aggregator	Aggregator
Transformation	application_source_qualifier	Application Source Qualifier

Object Type	Subtype Value	Description
Transformation	app_multi-group_source_qualifier	Application Multi-Group Source Qualifier
Transformation	custom_transformation	Custom
Transformation	custom_transformation	HTTP
Transformation	custom_transformation	SQL
Transformation	custom_transformation	Union
Transformation	custom_transformation	XML Generator
Transformation	custom_transformation	XML Parser
Transformation	expression	Expression
Transformation	external_procedure	External Procedure
Transformation	filter	Filter
Transformation	input_transformation	Input
Transformation	java	Java
Transformation	joiner	Joiner
Transformation	lookup_procedure	Lookup
Transformation	mq_source_qualifier	MQ Source Qualifier
Transformation	normalizer	Normalizer
Transformation	output_transformation	Output
Transformation	rank	Rank
Transformation	router	Router
Transformation	sequence	Sequence Generator
Transformation	sorter	Sorter
Transformation	source_qualifier	Source Qualifier
Transformation	stored_procedure	Stored Procedure
Transformation	transaction_control	Transaction Control
Transformation	update_strategy	Update Strategy
Transformation	xml_source_qualifier	XML Source Qualifier

## Auflisten von Ordnern

Verwenden Sie `ListObjects`, um jeden Ordner im Repository zurückzugeben. Wenn Sie als Objekttyp `Ordner` eingeben, ignoriert *pmrep* den Subtyp und den Ordnernamen.

Zum Auflisten aller Ordner im Repository verwenden Sie beispielsweise die folgende Syntax:

```
listobjects -o folder
```

Alternativ können Sie einen anderen Spaltentrenner und Listenende-Indikator eingeben:

```
ListObjects -o folder -c "***" -l #
```

## Auflisten von Objekten

Verwenden Sie `ListObjects`, um wiederverwendbare und nicht wiederverwendbare Objekte im Repository oder in einem Ordner aufzulisten. *pmrep* enthält keine Instanzen wiederverwendbarer Objekte. Wenn Sie Objekte auflisten, müssen Sie den Ordnernamen für alle Objekte einschließen, die einem Ordner zugeordnet sind.

*pmrep* gibt ggf. den Namen des Objekts mit dem Pfad zurück. Wenn beispielsweise ein Mapping oder Mapplet eine Transformation enthält, gibt *pmrep* *mapping\_name.transformation\_name* oder *mapplet\_name.transformation\_name* zurück.

Weitere Informationen zu einer Liste der Umwandlungs- oder Aufgaben-Rückgabewerte finden Sie unter ["Listing Object Types" auf Seite 1494](#).

Um beispielsweise alle Transformationstypen in einem Ordner aufzulisten, geben Sie den folgenden Text bei der Eingabeaufforderung ein:

```
listobjects -o transformation -f myfolder
```

*pmrep* gibt die folgenden Informationen zurück:

```
stored_procedure reusable sp_sproc1
expression reusable expl
stored_procedure non-reusable mapping1.sp_nsproc
sequence non-reusable smallmapplet.seqgen_empid
.listobjects completed successfully.
```

Um alle Transformationen einer gespeicherten Prozedur aufzulisten, geben Sie den folgenden Text bei der Eingabeaufforderung ein:

```
listobjects -o transformation -t stored_procedure -f myfolder
```

*pmrep* gibt die folgenden Informationen zurück:

```
stored_procedure reusable sp_sproc1
stored_procedure non-reusable mapping1.sp_nsproc
.listobjects completed successfully.
```

Um alle Sitzungen in einem Ordner aufzulisten, geben Sie den folgenden Text bei der Eingabeaufforderung ein:

```
listobjects -o session -f myfolder
```

*pmrep* gibt die folgenden Informationen zurück:

```
session reusable s_sales_by_CUSTID
session non-reusable wf_sales.s_sales_Q3
session non-reusable wf_orders.wl_shirt_orders.s_shirt_orders
.listobjects completed successfully.
```

# ListTablesBySess

Gibt eine Liste von Quellen und Targets zurück, die in einer Sitzung verwendet wurden. Wenn Sie Quellen oder Targets auflisten, gibt *pmrep* Quell- oder Target-Instanznamen im Fenster zurück. Verwenden Sie ListTablesBySess in einem Shell-Skript mit anderen *pmrep*-Befehlen. Sie können beispielsweise ein Shell-Skript erstellen, das ListTablesBySess zum Zurückgeben von Quellinstanznamen und Updatesrcprefix zum Aktualisieren des Quelleneigentümer-Namens verwendet.

Wenn Sie ListTablesBySess verwenden, gibt *pmrep* die Quell- und Target-Instanznamen wie sie in den Sitzungseigenschaften erscheinen zurück. Wenn beispielsweise das Mapping ein Mapplet mit einer Quelle enthält, gibt *pmrep* den Quellinstanznamen in folgendem Format zurück:

```
mapplet_name.source_name
```

Der ListTablesBySess-Befehl verwendet die folgende Syntax:

```
listtablesbysess  
  
-f <folder_name>  
  
-s [<qualifying_path>.]<session_name>  
  
-t <object_type_listed> (source or target)
```

In der folgenden Tabelle werden die *pmrep* ListTablesBySess-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-f	folder_name	Erforderlich. Name des Ordners, der die Sitzung enthält.
-s	session_name	Erforderlich. Name der Sitzung mit den Quellen oder Targets. Sie können einen wiederverwendbaren oder nicht wiederverwendbaren Sitzungsnamen eingeben. Sie können jedoch keine Instanz eines wiederverwendbaren Sitzungsnamens eingeben.  Um einen nicht wiederverwendbaren Sitzungsnamen in einem Arbeitsablauf einzugeben, geben Sie den Arbeitsablaufnamen und den Sitzungsnamen im Format <i>workflow_name.session_name</i> ein.
-t	object_type_listed	Erforderlich. Geben Sie Quelle zum Auflisten von Quellen oder Target zum Auflisten von Targets ein.

Um beispielsweise alle Quellen in einer wiederverwendbaren Sitzung aufzulisten, geben Sie den folgenden Text bei der Eingabeaufforderung ein:

```
listtablesbysess -f myfolder -s s_reus_sess1 -t source
```

*pmrep* gibt die folgenden Informationen zurück:

```
ITEMS  
mapplet1.ORDERS  
Shortcut_To_ITEM_ID  
listtablesbysess completed successfully.
```

Wenn das Mapping ein Mapplet mit einer Quelle beinhaltet, enthält *pmrep* den Mapplet-Namen mit der Quelle, z. B. mapplet1.ORDERS.

Sie können beispielsweise alle Targets in einer nicht wiederverwendbaren Sitzung in einem Arbeitsablauf auflisten:

```
listtablesbysess -f myfolder -s wf_workkflow1.s_nr_sess1 -t target
```

*pmrep* gibt die folgenden Informationen zurück:

```
target1_inst
ORDERS_BY_CUSTID
Shortcut_To_tgt2_inst
listtablesbysess_completed successfully.
```

## ListUserConnections

Listet die Informationen für jeden, mit dem Repository verbundenen Benutzer auf.

Der ListUserConnections-Befehl verwendet die folgende Syntax:

```
listuserconnections
```

## MassUpdate

Aktualisiert Sitzungseigenschaften für eine Reihe von Sitzungen, die angegebene Bedingungen erfüllen. Sie können alle Sitzungen in einem Ordner oder einer Liste von Sitzungen aktualisieren. Um eine Liste von Sitzungen zu aktualisieren, erstellen Sie eine persistente Eingabedatei. Die Liste kann eine bestimmte Liste von Sitzungen oder Bedingungen wie Namensmuster oder Eigenschaftswert enthalten. Verwenden Sie `ExecuteQuery`, um eine persistente Eingabedatei zu generieren.

Wenn Sie `MassUpdate` ausführen, können Sie Informationen wie den Ordernamen, die Anzahl der Sitzungen, die erfolgreich aktualisiert wurden oder fehlgeschlagen sind, und die Namen der aktualisierten Sitzungen anzeigen. Sie können den Status der Aktualisierung im Befehlszeilenfenster oder in einer vom Befehl generierten Protokolldatei anzeigen. Geben Sie den Namen und Pfad für die Protokolldatei ein, wenn Sie den Befehl ausführen. Standardmäßig wird die Protokolldatei in dem Verzeichnis gespeichert, in dem Sie den Befehl ausführen.

Verwenden Sie `MassUpdate` zum Aktualisieren einer Sitzungseigenschaft über mehrere Sitzungen, wenn eine PowerCenter Version einen Standardwert ändert.

**Hinweis:** Abhängige Sitzungseigenschaften können nicht aktualisiert werden.

Bevor Sie die Sitzungen aktualisieren, können Sie `MassUpdate` auch in einem Testmodus ausführen, um Änderungen anzuzeigen. Ein Beispiel einer Protokolldatei finden Sie auf ["Beispiel-Protokolldatei" auf Seite 1505](#).

Der `MassUpdate`-Befehl verwendet die folgende Syntax:

```
pmrep massupdate

-t <session_property_type (session_property, session_config_property,
transformation_instance_attribute, session_instance_runtime_option)>

-n <session_property_name>

-v <session_property_value>

[-w <transformation_type>]

{-i <persistent_input_file> | -f <folder_name> }

[-o <condition_operator (equal, unequal, less, greater)>]

[-l <condition_value>]
```

`[-g <update_session_instance_flag>]`

`[-m <test_mode>]`

`[-u <output_log_file_name>]`

In der folgenden Tabelle werden die *pmrep* MassUpdate-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-t	session_property_type	Erforderlich. Zu aktualisierender Sitzungseigenschaftstyp. Es gibt folgende Typen von Sitzungseigenschaften: <ul style="list-style-type: none"><li>- session_property</li><li>- session_config_property</li><li>- transformation_instance_attribute</li><li>- session_instance_runtime_option</li></ul>
-n	session_property_name	Erforderlich. Name des zu aktualisierenden Attributs oder der zu aktualisierenden Eigenschaft.
-v	session_property_value	Erforderlich. Wert (gefolgt von einem Semikolon), den Sie der Eigenschaft zuweisen möchten. Verwenden Sie zum Zuweisen eines Werts zur Eigenschaft beispielsweise folgende Syntax: -v "IgnoreNULLInExpressionComparison=Yes;" <b>Hinweis:</b> Setzen Sie den Sitzungseigenschaftswert in doppelte Anführungszeichen.
-w	transformation_type	Erforderlich, wenn Sie ein Umwandlungsinstanzattribut aktualisieren. Zu aktualisierender Umwandlungstyp. Sie können die folgenden Umwandlungstypen aktualisieren: Aggregat, Joiner, Lookup, Rang, Sortierer, Quelldefinition und Zieldefinition.
-i	persistent_input_file	Erforderlich, wenn Sie die Option -f nicht verwenden. Name der Datei, die die ausgewählte Liste der zu aktualisierenden Sitzungen enthält. Sie können mit dem <i>pmrep</i> ExecuteQuery-Befehl eine Abfrage ausführen und diese Datei generieren. MassUpdate gibt einen Fehler zurück, wenn Sie ein Objekt angeben, das keine Sitzung ist. Sie müssen die Option -i oder die Option -f verwenden, aber nicht beide.
-f	folder_name	Erforderlich, wenn Sie nicht die Option -i verwenden. Name des Ordners. Verwenden Sie diesen, um alle Sitzungen in einem Ordner zu aktualisieren. Sie müssen die Option -i oder die Option -f verwenden, aber nicht beide.
-o	condition_operator	Erforderlich, wenn Sie condition_value verwenden. Teil der Bedingung, die den Sitzungssatz definiert. Das Attribut einer Sitzung oder Sitzungsinstanz wird aktualisiert, wenn die Bedingung erfüllt ist. Sie können die folgenden Bedingungsoperatoren verwenden, um eine Zeichenfolge zu aktualisieren: gleich oder ungleich. Sie können die folgenden Bedingungsoperatoren verwenden, um eine Ganzzahl zu aktualisieren: gleich, ungleich, kleiner oder größer.



Option	Argument	Beschreibung
-l	condition_value	Erforderlich, wenn Sie einen Bedingungsoperator verwenden. Teil der Bedingung. Die Bedingung wird wie folgt angezeigt: <session_property_value> <condition operator> <condition_value>
-g	update_session_instance_flag	Erforderlich, wenn Sie die Laufzeioption einer Sitzungsinstanz aktualisieren. Optional bei folgenden Sitzungseigenschaftstypen: Sitzungseigenschaft, Sitzungskonfigurationsattribut und Umwandlungsinstanzattribut. Aktualisiert Sitzungsinstanzen. Sie können ein Attribut in einer Sitzungsinstanz aktualisieren, wenn die Sitzungsinstanz das Attribut überschreibt.
-m	test_mode	Optional. Führt MassUpdate im Testmodus aus. Zeigen Sie Sitzungen an, auf die sich der Befehl auswirkt, bevor Sie Änderungen vornehmen. Sie können die folgenden Details im Befehlszeilenfenster anzeigen: <ul style="list-style-type: none"> <li>- Sitzungsname</li> <li>- Sitzungstyp: wiederverwendbar oder nicht wiederverwendbar</li> <li>- Aktueller Wert der Sitzungseigenschaft</li> <li>- Sitzungen, bei denen das Attribut den gleichen Wert hat und auf die der Befehl keine Auswirkung hat.</li> </ul>
-u	output_log_file_name	Optional. Name der Protokolldatei, die den Status der Aktualisierung und Basisinformationen zu Sitzungen und Sitzungsinstanzen speichert. Vorherige Attributwerte werden ebenfalls in diese Datei geschrieben. Wenn Sie diese Option nicht verwenden, werden die Details im Befehlszeilenfenster angezeigt.

Der MassUpdate-Befehl gibt die Meldung "massupdate erfolgreich abgeschlossen" oder "Ausführen von massupdate fehlgeschlagen" zurück. Die Aktualisierung kann aus folgenden Gründen fehlschlagen:

- Sie haben keinen für den Attributnamen gültigen Attributwert angegeben.
- Sie haben den korrekten Namen der Sitzungseigenschaft zusammen mit dem falschen Sitzungseigenschafts-Typ angegeben.
- Sie haben die Option -v, die mit einem Semikolon endet, beim Aktualisieren eines Sitzungseigenschaftswert nicht angegeben.
- Sie haben während der Aktualisierung eines Transformationsinstanz-Attributs die Option -w nicht angegeben.
- Sie haben während der Aktualisierung einer Sitzungsinstanz-Laufzeioption die Option -g nicht angegeben.
- Sie verfügen nicht über die Repository Services-Administratorrolle.

## Sitzungseigenschafts-Typen

Wenn Sie MassUpdate ausführen, geben Sie den Sitzungseigenschafts-Typ und den Namen an. Sie legen folgende Sitzungseigenschafts-Typen fest:

- Sitzungseigenschaften
- Sitzungskonfigurationsattribute
- Transformationsinstanzattribute

- Sitzungsinstanz-Laufzeitoptionen

**Hinweis:** Sie müssen die Sitzungseigenschaft in Anführungszeichen einschließen.

In der folgenden Tabelle werden die aktualisierbaren Sitzungseigenschaften und die Sitzungseigenschaftstypen aufgelistet:

Sitzungseigenschaft	Sitzungseigenschafts-Typ
\$Quellenverbindungswert	session_property
\$Target-Verbindungswert	session_property
Zusätzliche gleichzeitige Pipelines für die Erstellung des Lookup-Cache	session_config_property
Größe des Aggregator-Datencaches	transformation_instance_attribute Das Argument transformation_type muss Aggregator sein.
Aggregator-Index - Cache-Größe	transformation_instance_attribute Das Argument transformation_type muss Aggregator sein.
Temporäre Sequenz für Pushdown zulassen	session_property
Temporäre Ansicht für Pushdown zulassen	session_property
Cache-Verzeichnis	transformation_instance_attribute Das Argument transformation_type muss Aggregator, Joiner oder Rang sein.
Cache-LOOKUP()-Funktion	session_config_property
Leistungsdaten erfassen	session_property
Commit-Intervall	session_property
Commit-Typ	session_property
Constraintbasierte Lastreihenfolge	session_config_property
Benutzerdefinierte Eigenschaften	session_config_property
DateTime-Format-String	session_config_property
Standard-Pufferblockgröße	session_config_property
Diese Aufgabe deaktivieren	session_instance_runtime_option
DTM-Puffergröße	session_property
Hohe Präzision aktivieren	session_property
Prüflast aktivieren	session_property
Übergeordnetes Objekt schlägt fehl, wenn diese Aufgabe nicht ausgeführt wird	session_instance_runtime_option

Sitzungseigenschaft	Sitzungseigenschafts-Typ
Übergeordnetes Objekt schlägt fehl, wenn diese Aufgabe fehlschlägt	session_instance_runtime_option
Inkrementelle Aggregation	session_property
Ist aktiviert	session_config_property
Java Klassenpfad	session_property
Joiner-Daten-Cachegröße	transformation_instance_attribute Das Argument transformation_type muss Joiner sein.
Joiner-Index-Cachegröße	transformation_instance_attribute Das Argument transformation_type muss Joiner sein.
Zeilensequenzielle Pufferlänge	session_config_property
Lookup-Cache-Verzeichnisname	transformation_instance_attribute Das Argument transformation_type muss Lookup-Prozedur sein.
Lookup-Daten-Cachegröße	transformation_instance_attribute Das Argument transformation_type muss Lookup-Prozedur sein.
Lookup-Index-Cachegröße	transformation_instance_attribute Das Argument transformation_type muss Lookup-Prozedur sein.
Maximal zulässige Speicherkapazität für automatische Speicherattribute	session_config_property
Maximaler Prozentsatz der zulässigen Gesamtspeicherkapazität für automatische Speicherattribute	session_config_property
Bei Fehler vor oder nach SQL	session_config_property
Bei Befehlsaufgabenfehler vor Sitzung	session_config_property
Bei Fehler in gespeicherter Prozedur	session_config_property
Ausgabedateiverzeichnis	transformation_instance_attribute Das Argument transformation_type muss Target-Definition sein.
Tracing überschreiben	session_config_property
Name der Parameterdatei	session_property
Zeitstempel für Kompatibilität vor 85	session_config_property
Zuvor erstellter Lookup-Cache	session_config_property
Pushdown-Optimierung	session_property

Sitzungseigenschaft	Sitzungseigenschafts-Typ
Rang-Daten-Cachegröße	transformation_instance_attribute Das Argument transformation_type muss Rang sein.
Rang-Index-Cachegröße	transformation_instance_attribute Das Argument transformation_type muss Rang sein.
Wiederherstellungsstrategie	session_property
Ablehnungsdateiverzeichnis	transformation_instance_attribute Das Argument transformation_type muss Target-Definition sein.
Transaktionen bei Fehlern rückgängig machen	session_property
Sitzungsprotokoll speichern nach	session_config_property
Sitzungsprotokolldatei-Verzeichnis	session_property
Erneuter Sitzungsversuch bei Deadlock	session_property
Sitzungs-Sortier-Reihenfolge	session_property Wenn der Integration Service im Unicode-Modus ausgeführt wird, können Sie die Sortierreihenfolge für das Sortieren von Zeichendaten in der Sitzung auswählen. Sie können die folgenden Werte für die Sortierreihenfolge konfigurieren: <ul style="list-style-type: none"> <li>- 0. BINARY</li> <li>- 2. SPANISH</li> <li>- 3. TRADITIONAL_SPANISH</li> <li>- 4. DANISH</li> <li>- 5. SWEDISH</li> <li>- 6. FINNISH</li> </ul>
Sortierer-Cachegröße	transformation_instance_attribute Das Argument transformation_type muss Sortierer sein.
Quelldateiverzeichnis	transformation_instance_attribute Das Argument transformation_type muss Quellddefinition sein.
Stoppen bei Fehlern	session_config_property
Quellzeilen behandeln als	session_property
Eingabe-Link behandeln als AND	session_instance_runtime_option
Rückwärtskompatible Sitzungsprotokolldatei schreiben	session_property

## Regeln und Richtlinien für MassUpdate

Verwenden Sie die folgenden Regeln und Richtlinien, wenn Sie MassUpdate ausführen:

- Wenn der Knoten, auf dem der Repository Service-Prozess ausgeführt wird, über begrenzte Speicherkapazität verfügt, deaktivieren Sie das Repository Agent Caching vor dem Ausführen von MassUpdate oder starten Sie den Repository Service nach dem Ausführen von MassUpdate.
- Sie können wiederverwendbare und nicht wiederverwendbare Sitzungen aktualisieren.
- Sie können den Wert einer unterstützten Sitzung oder die session config-Eigenschaft aktualisieren, unabhängig davon, ob sie überschrieben wird.
- Sie können nach dem Ausführen von MassUpdate Eigenschaftswerte nicht mehr umkehren.
- Ausgecheckte Sitzungen können nicht aktualisiert werden.
- Sitzungen in eingefrorenen Ordner können nicht aktualisiert werden.

## Beispiel-Protokolldatei

Der folgende Text zeigt ein Beispiel einer Protokolldatei, die von *pmrep* MassUpdate generiert wurde:

```
cases_auto,s_test_ff,reusable,0
s_test_ff was successfully checked out.

-----
11/10/2008 11:12:55 ** Saving... Repository test_ver_MU, Folder cases_auto
-----
Session s_test_ff updated.
Checking-in saved objects...done
-----

cases_auto,wf_non_reusable_test_ff.s_test_ff_non_reusable,non-reusable,0
wf_non_reusable_test_ff was successfully checked out.

-----
11/10/2008 11:12:57 ** Saving... Repository test_ver_MU, Folder cases_auto
-----
Validating the flow semantics of Workflow wf_non_reusable_test_ff...
...flow semantics validation completed with no errors.

Validating tasks of Workflow wf_non_reusable_test_ff...
...Workflow wf_non_reusable_test_ff tasks validation completed with no errors.

Workflow wf_non_reusable_test_ff updated.
Checking-in saved objects...done
-----

Massupdate Summary:
Number of reusable sessions that are successfully updated: 1.
Number of non-reusable sessions that are successfully updated: 1.
Number of session instances that are successfully updated: 0.
Number of reusable sessions that fail to be updated: 0.
Number of non-reusable sessions that fail to be updated: 0.
Number of session instances that fail to be updated: 0.
-----
```

## ModifyFolder

Ändert Ordneigenschaften. Sie ändern einen Ordner in einem nicht versionsgesteuerten Repository.

Der Befehl gibt "ModifyFolder erfolgreich abgeschlossen" oder "ModifyFolder fehlgeschlagen" zurück. Die Änderung schlägt möglicherweise aus folgenden Gründen fehl:

- Der Ordner existiert nicht.
- Die neue Eigentümer existiert nicht oder gehört nicht zur Gruppe.
- Ein Ordner mit dem neuen Ordnernamen ist bereits vorhanden.

Der ModifyFolder-Befehl verwendet die folgende Syntax:

```
modifyFolder
-n <folder_name>
[-d <folder_description>]
[-o <owner_name>]
[-a <owner_security_domain>]
[-s (shared folder)]
[-p <permissions>]
[-r <new_folder_name>]
[-f <folder_status> (active, frozendeploy, or frozennodeploy)]
[-u <os_profile>]
```

In der folgenden Tabelle werden die *pmrepModifyFolder* -Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-n	folder_name	Erforderlich. Neuer Ordnername.
-d	folder_description	Optional. Beschreibung des Ordners, der im Repository angezeigt wird.
-o	owner_name	Optional. Aktueller Eigentümer des Ordners. Jeder Benutzer im Repository kann Eigentümer des Ordners sein. Standardeigentümer ist der aktuelle Benutzer.
-a	owner_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Eigentümer gehört. Die Standardeinstellung ist "Native".
-s	shared_folder	Optional. Stellt den Ordner zur gemeinsamen Nutzung zur Verfügung.
-p	Berechtigungen	Optional. Zugriffsberechtigungen für den Ordner. Wenn dies ausgelassen wird, verwendet der Repository Service vorhandene Berechtigungen.
-r	new_folder_name	Optional. Neuer Name des Ordners.

Option	Argument	Beschreibung
-f	folder_status	Optional. Ändern Sie den Ordnerstatus auf einen der folgenden Status: <ul style="list-style-type: none"> <li>- active. Dieser Status ermöglicht Benutzern das Auschecken versionsgesteuerte Objekte im Ordner.</li> <li>- frozendeploy (Eingefroren, Ersetzen bei Bereitstellung zulassen). Dieser Status verhindert, dass Benutzer Objekte im Ordner auschecken. Bei der Bereitstellung im Ordner werden neue Versionen der Objekte erstellt.</li> <li>- frozenodeploy (Eingefroren, Ersetzen bei Bereitstellung nicht zulassen). Dieser Status verhindert, dass Benutzer Objekte im Ordner auschecken. Sie können in diesem Ordner keine Objekte bereitstellen.</li> </ul>
-u	os_profile	Optional. Weist dem Ordner ein Betriebssystemprofil zu.

## Benachrichtigen

Sendet Benachrichtigungsmeldungen an Benutzer, die mit einem Repository verbunden sind, oder an Benutzer, die mit allen von einem Repository Service verwalteten Repositories verbunden sind.

Der Notify-Befehl verwendet die folgende Syntax:

```
notify
-m <message>
```

In der folgenden Tabelle werden *pmrep* Notify-Option und -Argument beschrieben:

Option	Argument	Beschreibung
-m	message	Erforderlich. Meldung, die gesendet werden soll.

Der Befehl gibt "Notify erfolgreich abgeschlossen" oder "Ausführen von Notify fehlgeschlagen" zurück. Die Benachrichtigung schlägt möglicherweise aus folgenden Gründen fehl:

- Die von Ihnen eingegebene Meldung ist ungültig.
- Die Verbindung zum Repository Service wurde nicht hergestellt.
- Der Repository Service konnte Benutzer nicht benachrichtigen.

## ObjectExport

Exportiert Objekte in eine XML-Datei, die in der Datei powrmart.dtd definiert ist. Sie exportieren ein Objekt nach Name. Wenn Sie ein Objekt eingeben, müssen Sie den Namen des Ordners eingeben, der das Objekt enthält. Wenn Sie keine Versionsnummer eingeben, exportieren Sie die neueste Version des Objekts.

Verwenden Sie eine persistente Eingabedatei, um mehrere Objekte anzugeben, die gleichzeitig exportiert werden sollen. Sie können diese Datei mit den *pmrep*-Befehlen ExecuteQuery, Validate oder ListObjectDependencies erstellen. Wenn Sie die persistente Eingabedatei verwenden, benutzen Sie keine anderen Parameter zur Angabe von Objekten.

Wenn Sie ein Mapping exportieren, exportiert PowerCenter standardmäßig das Mapping mit den zugehörigen Instanzen. Wenn Sie abhängige Objekte einschließen möchten, müssen Sie die entsprechenden *pmrep*-Optionen hinzufügen. Optional können Sie wiederverwendbare und nicht wiederverwendbare abhängige Objekte, durch Shortcuts referenzierte Objekte sowie zugehörige Objekte in einer Primärschlüssel-Fremdschlüssel-Beziehung einschließen.

Zum Exportieren von Mapping-Abhängigkeiten müssen Sie die Optionen *-b* und *-r* verwenden.

Der ObjectExport-Befehl verwendet die folgende Syntax:

```
objectexport
{{-n <object_name>
-o <object_type>
[-t <object_subtype>]
[-v <version_number>]
[-f <folder_name>]} |
-i <persistent_input_file>}
[-m (export pk-fk dependency)]
[-s (export objects referred by shortcut)]
[-b (export non-reusable dependents)]
[-r (export reusable dependents)]
-u <xml_output_file_name>
[-l <log_file_name>]
[-e dbd_separator]
```

In der folgenden Tabelle werden die *pmrep* ObjectExport-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-n	object_name	Erforderlich, wenn Sie nicht die Option -i verwenden. Der Name eines bestimmten Objekts, das exportiert werden soll. Wenn Sie diese Option nicht eingeben, exportiert <i>pmrep</i> alle aktuellen oder ausgecheckten Objekte im Ordner. Verwenden Sie die Option -n oder -i, aber nicht beide.
-o	object_type	Objekttyp des Objektnamens. Sie können Quelle, Target, Transformation, Mapping, Mapplet, Sitzung, Worklet, Arbeitsablauf, Scheduler, Sitzungskonfiguration oder Aufgabe festlegen. Bei Verwendung dieser Option kann die Option -i nicht benutzt werden.
-t	object_subtype	Typ der Transformation oder Aufgabe. Dieses Argument wird bei anderen Objekttypen ignoriert. Weitere Informationen zu gültigen Subtypen finden Sie unter <a href="#">"Listing Object Types" auf Seite 1494</a> .
-v	version_number	Optional. Exportiert die Version des eingegebenen Objekts.
-f	folder_name	Name des Ordners, der das zu exportierende Objekt enthält. Wenn Sie keinen Objektnamen eingeben, exportiert <i>pmrep</i> alle Objekte in diesem Ordner. Bei Verwendung dieser Option kann die Option -i nicht benutzt werden.



Option	Argument	Beschreibung
-i	persistent_input_file	Erforderlich, wenn Sie die Option -n nicht verwenden. Textdateiliste der Objekte, die mit ExecuteQuery, Validate oder ListObjectDependencies generiert wurden. Sie enthält Objektdatensätze mit kodierten IDs. Wenn Sie diesen Parameter verwenden, können Sie die Optionen -n, -o und -f nicht benutzen.
-m	-	Erforderlich zum Exportieren abhängiger Objekte. Exportiert Primärschlüssel-Tabellendefinitionen beim Exportieren von Quellen und Targets mit Fremdschlüsseln.
-s	-	Erforderlich zum Exportieren abhängiger Objekte. Exportiert das ursprüngliche, vom Shortcut referenzierte Objekt.
-b	-	Erforderlich zum Exportieren abhängiger Objekte. Exportiert vom Objekt benutzte, nicht wiederverwendbare Objekte.
-r	-	Erforderlich zum Exportieren abhängiger Objekte. Exportiert vom Objekt benutzte, wiederverwendbare Objekte.
-u	xml_output_file_name	Erforderlich. Name der XML-Datei, die die Objektinformationen enthalten soll.
-l	log_file_name	Optional. Protokolldatei, die alle Exportschritte aufzeichnet. Wenn Sie diese Option auslassen, werden im Fenster Statusmeldungen ausgegeben.
-e	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name\source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.

## Beispiele

Das folgende Beispiel exportiert ein Mapping mit dem Namen "Map", das in folder1 gespeichert ist, in eine Datei mit dem Namen map.xml:

```
objectexport -n map -o mapping -f folder1 -u map.xml
```

Das folgende Beispiel exportiert die Objekte in einer persistenten Eingabedatei mit dem Namen persistent\_input.xml in eine Datei mit dem Namen map.xml:

```
objectexport -i persistent_input.txt -u map.xml
```

**Hinweis:** Wenn Sie eine manuell erstellte persistente Eingabedatei verwenden, wird folgende Meldung angezeigt, da Sie als kodierte ID "none" eingegeben haben: IDs sind ungültig. Versuch mit Namen für [none,folder1,map,mapping,none,1].

## ObjectImport

Importiert Objekte aus einer XML-Datei. Dieser Befehl erfordert eine Steuerdatei, um die zu importierenden Objekte und die Konfliktlösungsmethode festzulegen. Die Steuerdatei ist eine XML-Datei, die durch die Datei „impcntl.dtd“ definiert wird.

Der ObjectImport-Befehl verwendet die folgende Syntax:

```
objectimport  
-i <input_xml_file_name>  
-c <control_file_name>  
[-l <log_file_name>]  
[-p (retain persistent value)]
```

In der folgenden Tabelle werden die *pmrep* ObjectImport-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-i	input_XML_file_name	Erforderlich. Name der zu importierenden XML-Datei.
-c	control_file_name	Erforderlich. Name der Steuerdatei, die Importoptionen definiert.
-l	log_file_name	Optional. Protokolldatei, die alle Exportschritte aufzeichnet. Wenn Sie diese Option auslassen, werden im Fenster Statusmeldungen ausgegeben.
-p	-	Optional. Behält persistente Werte für Mapping-Variablen bei.

**Hinweis:** Der ObjectImport-Befehl erstellt keinen Ordner, wenn der eingegebene Ordnername nicht im Repository existiert.

Sie können Audit-Protokolle generieren, wenn Sie eine XML-Datei mit dem Befehl „pmrep ObjectImport“ in das PowerCenter-Repository importieren. Wenn Sie ein oder mehrere Repository-Objekte importieren, können Sie Audit-Protokolle generieren. Um Sicherheits-Audit-Trails in die Protokollereignisse für Benutzeraktivitäten aufzunehmen, aktivieren Sie vor dem Import einer XML-Datei die Eigenschaft „SecurityAuditTrail“ für den PowerCenter-Repository-Dienst im Administrator Tool. Die Benutzeraktivitätsprotokolle erfassen alle Audit-Meldungen.

Die Audit-Protokolle enthalten die folgenden Informationen über die importierten XML-Dateien:

- Hostname und IP-Adresse des Clientcomputers, von dem aus die XML-Datei importiert wurde
- Vollständigen lokalen Pfad der XML-Importdatei
- Dateiname
- Dateigröße in Byte
- Name des angemeldeten Benutzers
- Anzahl der importierten Objekte
- Zeitstempel des Importvorgangs

## PurgeVersion

Bereinigt Objektversionen von der Repository-Datenbank. Sie können Versionen gelöschter Objekte und aktiver Objekte bereinigen. Ein Objekt ist ein gelöschttes Objekt, wenn die neueste Version eing\_checked ist und den Gelöscht-Versionsstatus aufweist. Andere Objekte sind aktive Objekte.

Wenn Sie Versionen gelöschter Objekte bereinigen, werden alle Versionen bereinigt. Die gelöschten Objekte müssen eing\_checked werden. Sie können Versionen für alle gelöschten Objekte bereinigen oder für Objekte,

die vor einem angegebenen Endzeitpunkt gelöscht wurden. Sie können die Endzeit als Datum und Uhrzeit, nur als Datum oder als Anzahl von Tagen vor dem aktuellen Datum festlegen.

Wenn Sie Versionen aktiver Objekte bereinigen, können Sie Bereinigungskriterien angeben. Sie können die Anzahl der beizubehaltenden Versionen festlegen und frühere Version bereinigen oder Sie bereinigen Versionen, die älter sind als ein festgelegter Cutoff-Zeitpunkt. Sie können weder eine ausgecheckte Version noch die aktuellste eingeecheckte Version bereinigen.

Wenn Sie Versionen eines Verbundobjekts bereinigen, achten Sie darauf, welche Versionen der abhängigen Objekte bereinigt werden.

Mit der Option `-k` können Sie die Objekte, die nicht bereinigt werden, sowie den Grund dafür anzeigen, warum Objektversionen nicht bereinigt werden. Sie verfügen beispielsweise nicht über die Berechtigung zum Bereinigen einer Objektversion. Sie können Objektversionen, die zu einer Bereitstellungsgruppe gehören, nicht bereinigen.

Der `PurgeVersion`-Befehl verwendet die folgende Syntax:

```
purgeversion
{-d <all | time_date | num_day> |
{-n <last_n_versions_to_keep> |
-t <time_date | num_day>}}
[-f <folder_name>]
[-q <query_name>]
[-o <output_file_name>]
[-p (preview purged objects only)]
[-b (verbose)]
[-c (check deployment group reference)]
[-s dbd_separator]
[-k (log objects not purged)]
```

In der folgenden Tabelle werden die *pmrep* `PurgeVersion`-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-d	alle time_date num_day	Erforderlich, wenn Sie weder <code>-n</code> noch <code>-t</code> verwenden. Bereinigt alle Versionen der eingeecheckten gelöschten Objekte. Sie können <code>all</code> für alle gelöschten Objekte festlegen oder eine Endzeit angeben, um alle Versionen von Objekten zu bereinigen, die vor diesem Zeitpunkt gelöscht wurden. Legen Sie den Endzeitpunkt im Format MM/DD/YYYY HH24:MI:SS, im Format MM/DD/YYYY oder als Anzahl an Tagen vor dem aktuellen Datum fest. Wenn Sie eine Anzahl an Tagen angeben, muss der Wert eine Ganzzahl größer 0 sein.
-n	last_n_versions_to_keep	Erforderlich, wenn Sie <code>-d</code> oder <code>-t</code> nicht verwenden. Anzahl der neuesten eingeecheckten Objektversionen, die für ein aktives Objekt beibehalten werden sollen. Der Wert muss eine Ganzzahl größer 0 sein. Geben Sie beispielsweise 6 ein, um alle Versionen außer den letzten sechs eingeecheckten Versionen zu bereinigen. Wenn das Objekt ausgecheckt ist, wird auch die ausgecheckte Version beibehalten. <b>Hinweis:</b> Nachdem Sie Objektversionen bereinigt haben, können Sie diese nicht mehr abrufen. Um sicherzustellen, dass Sie zu früheren Versionen zurückkehren können, sollten Sie nicht alle Versionen eines Objekts bereinigen.

Option	Argument	Beschreibung
-t	purge_cutoff_time	Erforderlich, wenn Sie -d oder -n nicht verwenden. Cutoff-Zeitpunkt für das Bereinigen von Objektversionen von aktiven Objekten. Bereinigt Versionen, die vor dem Cutoff-Zeitpunkt eingecheckt wurden. Sie können den Cutoff-Zeitpunkt zum Bereinigen im Format MM/DD/YYYY HH24:MI:SS, im Format MM/DD/YYYY oder als Anzahl an Tagen vor dem aktuellen Datum festlegen. Wenn Sie eine Anzahl an Tagen angeben, muss der Wert eine Ganzzahl größer 0 sein. Wenn Sie die Option -t verwenden, behalten Sie die neueste eingecheckte Version, auch wenn diese nach dem Cutoff-Zeitpunkt zum Bereinigen eingecheckt wurde.
-f	folder_name	Optional. Ordner, auf dem Objektversionen bereinigt werden. Wenn Sie keinen Ordner festlegen, bereinigen Sie Objektversionen auf allen Ordnern im Repository.
-q	query_name	Optional. Abfrage zum Bereinigen von Objektversionen von einem bestimmten Abfrageergebnissatz. <b>Hinweis:</b> Wenn Sie die Option -d verwenden, bereinigen Sie alle Versionen der gelöschten Objekte. Um die neueren Versionen der gelöschten Objekte beizubehalten und ältere Versionen zu bereinigen, können Sie eine Abfrage definieren, die die gelöschten Objekte zurückgibt, und dann die Option -q zusammen mit -n, -t oder beidem verwenden.
-o	outputfile_name	Optional. Ausgabedatei zum Speichern von Informationen zu bereinigten Objektversionen.
-p	-	Optional. Zeigt eine Vorschau des PurgeVersion-Befehls an. <i>pmrep</i> zeigt die Bereinigungsergebnisse an, ohne die Objektversionen tatsächlich zu bereinigen.
-b	-	Optional. Zeigt oder speichert Bereinigungsinformationen im Verbose-Modus. Verbose-Modus bietet ausführliche Informationen zu Objektversionen, einschließlich Repository-Name, Ordner-Name, Versionsnummer und Status. Sie können die Option -b mit -o und -p verwenden.
-c	-	Optional. Prüft Bereitstellungsgruppen im Repository auf Verweise zu den Objektversionen, die in einer Bereinigungsvorschau zurückgegeben werden. Wenn in einer Bereinigungsvorschau eine Objektversion in einer Bereitstellungsgruppe enthalten ist, zeigt <i>pmrep</i> eine Warnung an. Wenn Sie die Option -c mit der Option -p verwenden, listet der Befehl Objekte auf, die bereinigt werden. Anschließend werden die Objektversionen aufgelistet, die in Bereitstellungsgruppen enthalten sind. Wenn Sie die Option -c ohne die Option -p verwenden, bereinigt der Befehl keine Objektversionen, die zu Bereitstellungsgruppen gehören. <b>Hinweis:</b> Die Option -c kann sich negativ auf die Leistung auswirken.

Option	Argument	Beschreibung
-s	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name \source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.
-k	-	Optional. Listet alle Objektnamen und Versionen auf, die nicht bereinigt werden, obwohl sie den Bereinigungskriterien entsprechen. Die Option -k listet auch den Grund dafür auf, warum die Objektversionen nicht bereinigt werden. Beispiel: Eine Objektversion wird nicht bereinigt, wenn Sie nicht über ausreichende Berechtigungen zum Löschen des Objekts verfügen. <b>Hinweis:</b> Eine Objektversion wird nicht bereinigt, wenn sie zu einer Bereitstellungsgruppe gehört. Wenn ein Objekt zu mehr als einer Bereitstellungsgruppe gehört, wird als Ursache für die Nichtbereinigung des Objekts die erste Bereitstellungsgruppe angeführt.

## Beispiele

Das folgende Beispiel bereinigt sämtliche Versionen aller gelöschten Objekte im Repository:

```
pmrep purgeversion -d all
```

**Hinweis:** Eine optimale Leistung erreichen Sie, indem Sie auf Ordnebene bereinigen oder Bereinigungskriterien verwenden, die die Anzahl der gelöschten Objektversionen reduzieren. Vermeiden Sie das Bereinigen aller gelöschten Objekte oder aller älteren Versionen auf Repository-Ebene.

Das folgende Beispiel bereinigt alle Objekte im Ordner folder1, mit Ausnahme der neuesten eingescheckten Objektversion:

```
pmrep purgeversion -n 1 -f folder1
```

Das folgende Beispiel zeigt eine Bereinigungsvorschau aller Objektversionen an, die vor Mittag des 5. Januar 2005 eingescheckt wurden, und gibt die Ergebnisse in der Datei mit dem Namen purge\_output.txt aus:

```
pmrep purgeversion -t '01/05/2005 12:00:00' -o purge_output.txt -p
```

## Register

Registriert ein lokales Repository bei einem verbundenen globalen Repository. Sie müssen eine Verbindung zum globalen Repository herstellen, bevor Sie das lokale Repository registrieren.

Außerdem müssen Sie den Repository Service für das lokale Repository im exklusiven Modus ausführen. Sie können die Ausführung des Repository Service im exklusiven Modus im Administrator-Tool konfigurieren oder den Befehl *infacmd* UpdateRepositoryService verwenden.

Der Befehl gibt "Register erfolgreich abgeschlossen" oder "Ausführen von Register fehlgeschlagen" zurück. Die Registrierung schlägt möglicherweise aus folgenden Gründen fehl:

- Die Verbindung zum Repository Service wurde nicht hergestellt.
- Das lokale Repository wird nicht im exklusiven Modus ausgeführt.
- Der Repository Service konnte Informationen zum globalen Repository nicht initialisieren.

- Der Repository Service konnte das lokale Repository nicht bei dem globalen Repository registrieren.

Der Register-Befehl verwendet die folgende Syntax:

```
register
-r <local_repository_name>
-n <local_repository_user_name>
[-s <local_repository_user_security_domain>]
[-x <local_repository_password> |
-X <local_repository_password_environment_variable>]
[-d <local_repository_domain_name> |
-h <local_repository_portal_host_name>
-o <local_repository_portal_port_number>]] (if local repository is in a different domain)
```

In der folgenden Tabelle werden die *pmrep* Register-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-r	local_repository_name	Erforderlich. Name des zu registrierenden lokalen Repository.
-n	local_repository_user_name	Erforderlich. Lokaler Benutzernamen.
-s	local_repository_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Die Standardeinstellung ist "Native".
-x	local_repository_password	Optional. Anmelde-Passwort für das lokale Target-Repository. Verwenden Sie die Option -x oder -X, aber nicht beide. Wenn Sie weder die Option -x noch -X verwenden, werden Sie von <i>pmrep</i> aufgefordert, das Passwort einzugeben.
-X	repository_password_environment_variable	Optional. Anmelde-Passwort-Umgebungsvariable für das lokale Target-Repository. Verwenden Sie die Option -x oder -X, aber nicht beide. Wenn Sie weder die Option -x noch -X verwenden, werden Sie von <i>pmrep</i> aufgefordert, das Passwort einzugeben.
-d	local_repository_domain_name	Erforderlich, wenn sich das lokale Repository in einer anderen Domäne befindet und Sie nicht die Optionen -h und -o verwenden. Name der Informatica-Domäne für das Repository.
-h	local_repository_portal_host_name	Erforderlich, wenn sich das lokale Repository in einer anderen Domäne befindet und Sie nicht die Option -d verwenden. Computernamen der Domäne, auf der das lokale Repository gespeichert ist. Wenn Sie diese Option verwenden, müssen Sie auch die Option -o benutzen.
-o	local_repository_portal_port_number	Erforderlich, wenn sich das lokale Repository in einer anderen Domäne befindet und Sie nicht die Option -d verwenden. Portnummer der Domäne, auf der das lokale Repository gespeichert ist. Wenn Sie diese Option verwenden, müssen Sie auch die Option -h verwenden.

# RegisterPlugin

Registriert ein externes Plug-In in einem Repository. Das Registrieren eines Plug-Ins fügt dessen Funktionalität dem Repository hinzu. Verwenden Sie den RegisterPlugin-Befehl zum Aktualisieren vorhandener Plug-Ins.

Wenn Sie diesen Befehl verwenden, muss der Repository Service im exklusiven Modus ausgeführt werden. Sie können die Ausführung des Repository Service im exklusiven Modus im Administrator-Tool konfigurieren oder den Befehl *infacmd* UpdateRepositoryService verwenden.

Der RegisterPlugin-Befehl verwendet die folgende Syntax:

```
registerplugin
-i <input_registration_file_name_or_path>
[-e (update plug-in)]
[-l <NIS_login>
  {-w <NIS_password> |
  -W <NIS_password_environment_variable>}
  [-k (CRC check on security library)]]
[-N (is native plug-in)]
```

In der folgenden Tabelle werden die *pmrep* RegisterPlugin-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-i	input_registration_file_name_or_path	Erforderlich. Name oder Pfad der Registrierungsdatei für das Plug-In.
-e	-	Optional. Aktualisieren Sie ein vorhandenes Plug-In. Nicht anwendbar bei Authentifizierungsmodulen.
-l	NIS login	Optional. Registriert Sicherheitsmodul-Komponenten. Stellen Sie die NIS-Anmeldung des Benutzers zur Verfügung, der ein externes Sicherheitsmodul registriert. Wenn das Plug-In ein Authentifizierungsmodul enthält, müssen Sie den externen Anmeldenamen angeben, andernfalls schlägt die Registrierung fehl. Diese Anmeldung wird als Administrator-Benutzername im Repository verwendet. Verwenden Sie diese Option nicht für andere Plug-Ins.
-w	NIS password	Optional. Verwenden Sie dies zum Registrieren von Authentifizierungsmodul-Komponenten. Passwort für externes Verzeichnis des Benutzers, der das Modul registriert. Wenn das Plug-In ein Authentifizierungsmodul enthält, müssen Sie das Benutzerpasswort des externen Verzeichnisses angeben, andernfalls schlägt die Registrierung fehl. Verwenden Sie diese Option nicht für andere Plug-Ins. Verwenden Sie die Option -w oder -W, aber nicht beide. Wenn Sie kein Passwort oder keine Passwort-Umgebungsvariable angeben, werden Sie von <i>pmrep</i> aufgefordert, das Passwort einzugeben.

Option	Argument	Beschreibung
-W	NIS_password_environment_variable	Optional. Verwenden Sie dies zum Registrieren von Authentifizierungsmodul-Komponenten. Passwort-Umgebungsvariable für externes Verzeichnis des Benutzers, der das Modul registriert. Wenn das Plug-In ein Authentifizierungsmodul enthält, müssen Sie das Benutzerpasswort des externen Verzeichnisses angeben, andernfalls schlägt die Registrierung fehl. Verwenden Sie diese Option nicht für andere Plug-Ins. Verwenden Sie die Option -w oder -W, aber nicht beide. Wenn Sie kein Passwort oder keine Passwort-Umgebungsvariable angeben, werden Sie von <i>pmrep</i> aufgefordert, das Passwort einzugeben.
-k	-	Optional. Speichert das CRC der Plug-In-Bibliothek im Repository. Wenn der Repository Service das Modul lädt, führt dieses eine CRC-Prüfung in der Bibliothek aus.
-N	-	Registriert ein Plug-In. Erforderlich, wenn die folgenden Bedingungen gegeben sind: <ul style="list-style-type: none"> <li>- Sie führen ein PowerCenter-Upgrade aus.</li> <li>- Das PowerCenter-Upgrade hat keine neue Repository-Version.</li> <li>- Das Plug-In enthält aktualisierte Funktionen.</li> <li>- Das Plug-In wird standardmäßig bei einer neuen PowerCenter-Installation registriert.</li> </ul>

## Registrieren eines Sicherheitsmoduls

Wenn Sie Benutzer und Passwörter für ein Repository mit einem externen Verzeichnisdienst verwalten möchten, müssen Sie das Sicherheitsmodul bei dem Repository registrieren. Verwenden Sie den Registerplugin-Befehl zum Registrieren des Sicherheits-Plug-Ins.

## Beispiel

Sie verwalten PowerCenter für eine Organisation, die ein zentralisiertes LDAP NIS zur Benutzerauthentifizierung hat. Bei der Ausführung eines PowerCenter-Upgrades entscheiden Sie sich, LDAP für die Benutzerauthentifizierung zu verwenden. Das Upgrade installiert das LDAP-Sicherheitsmodul im Repository-Sicherheitsordner. Nachdem der Connect-Befehl eine Verbindung zum Repository hergestellt hat, führt der Administrator den *pmrep*-Befehl zum Registrieren des neuen externen Moduls bei dem Repository aus:

```
pmrep registerplugin -i security/ldap_authen.xml -l adminuser -w admpass
```

Die Optionen -l für den Anmeldenamen und -w für das Anmelde-Passwort enthalten die gültigen NIS-Anmeldeinformationen für den Benutzer, der den *pmrep*-Befehl ausführt. Nach der Registrierung müssen Sie diesen Anmeldenamen und das Passwort für den Zugriff auf das Repository verwenden.

**Hinweis:** Der Anmelde-name und das Passwort müssen im externen Verzeichnis Gültigkeit haben, andernfalls kann der Administrator nicht mit LDAP auf das Repository zugreifen.

Die Option -i enthält den XML-Dateinamen, der das Sicherheitsmodul angibt.



# Wiederherstellen

Stellt eine Repository-Backup-Datei in einer Datenbank wieder her. Die Target-Datenbank muss leer sein.

Der *pmrep* Restore-Befehl verwendet die folgende Syntax:

```
restore
-u <domain_user_name>
[-s <domain_user_security_domain>]
[-p <domain_password> |
-P <domain_password_environment_variable>]
-i <input_file_name>
[-g (create global repository)]
[-y (enable object versioning)]
[-b (skip workflow and session logs)]
[-j (skip deployment group history)]
[-q (skip MX data)]
[-f (skip task statistics)]
[-a (as new repository)]
[-e (exit if domain name in the binary file is different from current domain name)]
```

In der folgenden Tabelle werden die *pmrep* Restore-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-u	domain_user_name	Erforderlich. Benutzername.
-s	domain_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Standardwert ist "Native".
-p	domain_password	Optional. Passwort. Sie können die Option -p oder -P verwenden, aber nicht beide. Wenn Sie weder die Option -p noch -P verwenden, werden Sie von <i>pmrep</i> aufgefordert, das Passwort einzugeben.
-P	domain_password_environment_variable	Optional. Passwort-Umgebungsvariable. Sie können die Option -p oder -P verwenden, aber nicht beide. Wenn Sie weder die Option -p noch -P verwenden, werden Sie von <i>pmrep</i> aufgefordert, das Passwort einzugeben.
-i	input_file_name	Erforderlich. Name der Repository-Backup-Datei. Verwenden Sie einen lokalen Dateinamen und Pfad des Repository Service.
-g	-	Optional. Stuft das Repository zu einem globalen Repository hoch.
-y	-	Optional. Ermöglicht Objektversionierung für das Repository.

Option	Argument	Beschreibung
-b	-	Optional. Überspringt beim Wiederherstellen Tabellen, die sich auf Arbeitsablauf und Sitzungsprotokolle beziehen.
-j	-	Optional. Überspringt beim Wiederherstellen die Bereitstellungsgruppen-Historie.
-q	-	Optional. Überspringt beim Wiederherstellen Tabellen, die sich auf MX-Daten beziehen.
-f	-	Optional. Überspringt beim Wiederherstellen Aufgabenstatistiken.
-a	-	Optional. Erstellt neue interne Ordner-IDs für Ordner im wiederhergestellten Repository. Dies ermöglicht Ihnen das Kopieren von Ordnern und Bereitstellungsgruppen zwischen dem ursprünglichen Repository und dem wiederhergestellten Repository. Wenn Sie nicht -a verwenden, können Sie keine Ordner und Bereitstellungsgruppen zwischen dem ursprünglichen und dem wiederhergestellten Repository kopieren.
-e	-	Optional. Abbruch, wenn der Domänenname in der Binärdatei vom aktuellen Domänennamen abweicht.

## Beispiel

Das folgende Beispiel stellt ein Repository als versionsgesteuertes Repository wieder her und gibt den Benutzernamen und das Passwort des Administrators an, um die Registrierung des LDAP-Sicherheitsmoduls beizubehalten:

```
restore -u administrator -p password -i repository1_backup.rep -y
```

## RollbackDeployment

Führt ein Rollback für eine Bereitstellung aus, um bereitgestellte Versionen von Objekten aus dem Target-Repository zu löschen. Verwenden Sie diesen Befehl zum Rollback für alle Objekte in einer Bereitstellungsgruppe, die Sie zu einem bestimmten Zeitpunkt (Datum und Uhrzeit) bereitgestellt haben.

Ein Rollback kann nicht nur für einen Teil der Bereitstellung durchgeführt werden. Um ein Rollback auszuführen, müssen Sie eine Verbindung zum Target-Repository herstellen. Sie können kein Rollback einer Bereitstellung von einem nicht versionsgesteuerten Repository ausführen.

Um ein Rollback zu initiieren, müssen Sie die aktuelle Version jedes Objekts für das Rollback verwenden.

Der RollbackDeployment-Befehl verwendet die folgende Syntax:

```
pmrep rollbackdeployment -p <deployment_group_name> -t <nth_latest_deploy_run> -r  
<repository_name> -v <nth_latest_version_of_deployment_group>
```

In der folgenden Tabelle werden die *pmrep*-RollbackDeployment-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-p	deployment_group_name	Erforderlich. Name der Bereitstellungsgruppe, für die ein Rollback ausgeführt werden soll.
-t	nth_latest_deploy_run	Erforderlich. Version der Bereitstellung, für die ein Rollback ausgeführt werden soll.
-r	repository_name	Optional. Name des Quellen-Repositorys, aus dem Sie die Bereitstellungsgruppe bereitstellen.
-v	nth_latest_version_of_deployment_group	Optional. Version der Bereitstellungsgruppe, für die ein Rollback ausgeführt werden soll.

## Beispiel

Sie haben eine Bereitstellung mit fünf Versionen und möchten ein Rollback für die letzten zwei Versionen durchführen. Dazu müssen Sie zuerst ein Rollback der neuesten Bereitstellung ausführen. Geben Sie den folgenden Text bei der Eingabeaufforderung ein, um ein einzelnes Rollback auszuführen und die letzte Bereitstellung zu bereinigen:

```
rollbackdeployment -p Deploy_sales -t 1
```

Geben Sie anschließend folgenden Text ein, um ein Rollback der vorletzten Bereitstellung durchzuführen:

```
rollbackdeployment -p Deploy_sales -t 2
```

## Ausführen

Öffnet eine Skriptdatei mit mehreren *pmrep*-Befehlen, liest die einzelnen Befehle und führt diese aus. Wenn die Skript-Datei mit UTF-8 kodiert ist, müssen Sie die Option -u verwenden und die Repository-Codepage muss UTF-8-kodiert sein. Wenn Sie eine mit UTF-8 kodierte Skriptdatei ausführen, die den Connect-Befehl für ein Repository beinhaltet, das keine UTF-8-Codepage aufweist, schlägt der Run-Befehl fehl.

Wenn die Skriptdatei nicht mit UTF-8 kodiert ist, lassen Sie die Option -u aus. Wenn Sie die Option -o und die Option -u verwenden, generiert *pmrep* die Ausgabedatei in UTF-8. Wenn Sie die Option -o verwenden und die Option -u auslassen, generiert *pmrep* die Ausgabedatei basierend auf dem Systemgebietsschema des Computers, auf dem Sie *pmrep* ausführen.

Der Befehl gibt "Run erfolgreich abgeschlossen" oder "Run fehlgeschlagen" aus. Die Ausführung schlägt möglicherweise fehl, wenn der Repository Service die Skriptdatei oder Ausgabedatei nicht öffnen kann.

Der Run-Befehl verwendet die folgende Syntax:

```
run
-f <script_file_name>
[-o <output_file_name>]
[-e (echo commands)]
[-s (stop at first error)]
[-u (UTF-8 encoded script file and output file)]
```

In der folgenden Tabelle werden die *pmrep* Run-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-f	script file name	Erforderlich. Name der Skriptdatei
-o	Ausgabedateiname	Optional. Name der Ausgabedatei. Diese Option schreibt alle Meldungen, die von den Befehlen in der Skriptdatei generiert wurden, in die Ausgabedatei. Wenn Sie die Option -u und die Option -o verwenden, generiert <i>pmrep</i> eine mit UTF-8 kodierte Ausgabedatei. Wenn Sie die Option -o ohne die Option -u verwenden, kodiert <i>pmrep</i> die Ausgabedatei basierend auf dem Systemgebietsschema des Computers, der <i>pmrep</i> ausführt.
-e	-	Optional. Befehle werden im Skript wiedergegeben.
-s	-	Optional. Stoppt die Skriptaufführung nach dem ersten Fehler.
-u	-	Optional. Kodiert die Ausgabedatei im UTF-8-Format. Wenn Sie die Option -u und die Option -o verwenden, kodiert <i>pmrep</i> auch die Ausgabedatei im UTF-8-Format. Verwenden Sie diese Option nur, wenn die Repository-Codepage UTF-8-kodiert ist.

## ShowConnectionInfo

Gibt den Repository-Namen und Benutzerinformationen für die aktuelle Verbindung zurück.

Verwenden Sie den ShowConnectionInfo-Befehl im interaktiven Modus. Wenn Sie eine Verbindung zu einem Repository im interaktiven Modus herstellen, speichert *pmrep* die Verbindungsinformationen bis Sie das Repository beenden oder eine Verbindung zu einem anderen Repository herstellen.

Wenn Sie den ShowConnectionInfo-Befehl im Befehlszeilenmodus verwenden, wird eine Meldung angezeigt, dass der Befehl nicht ausgeführt werden konnte. *pmrep* behält keine Verbindungsinformationen im Befehlszeilenmodus bei. Der ShowConnectionInfo-Befehl stellt keine Verbindung zum Repository her.

Der ShowConnectionInfo-Befehl verwendet die folgende Syntax:

```
showconnectioninfo
```

Er gibt Informationen zurück, die wie folgt aussehen können:

```
Connected to Repository MyRepository in MyDomain as user MyUserName
```

## SwitchConnection

Ändert den Namen einer vorhandenen Verbindung. Wenn Sie SwitchConnection verwenden, ersetzt der Repository Service die relationalen Datenbankverbindungen für alle Sitzungen, die die Verbindung an einem der folgenden Speicherorte verwenden:

- Quellverbindung
- Target-Verbindung
- Verbindungsinformations-Eigenschaft in Lookup-Transformationen
- Verbindungsinformations-Eigenschaft in Transformationen einer gespeicherten Prozedur

- \$Quellenverbindungswert-Sitzungseigenschaft
- \$Target-Verbindungswert-Sitzungseigenschaft

Wenn das Repository sowohl relationale Verbindungen als auch Anwendungsverbindungen mit dem gleichen Namen enthält und Sie den Verbindungstyp als relational in *allen* Speicherorten im Repository angeben, ersetzt der Repository Service die relationale Verbindung.

Beispiel: Sie haben eine relationale und eine Anwendungsquelle, beide mit der Bezeichnung ITEMS. In einer Sitzung haben Sie einer relationalen Quellverbindung den Namen ITEMS statt Relational:ITEMS gegeben. Wenn Sie SwitchConnection zum Ersetzen der relationale Verbindung ITEMS durch eine andere relationale Verbindung verwenden, ersetzt *pmrep* keine relationale Verbindung im Repository, weil es keinen Verbindungstyp für die Quellverbindung mit der Bezeichnung ITEMS bestimmen kann.

Der SwitchConnection-Befehl verwendet die folgende Syntax:

```
switchconnection
-o <old_connection_name>
-n <new_connection_name>
```

In der folgenden Tabelle werden die *pmrep* SwitchConnection-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	old_connection_name	Erforderlich. Name der zu ändernden Verbindung.
-n	new_connection_name	Erforderlich. Name der neuen Verbindung.

## TruncateLog

Löscht Details aus dem Repository. Sie können alle Protokolle oder Protokolle für einen Ordner oder einen Arbeitsablauf löschen. Sie können auch ein Datum eingeben und alle Protokolle löschen, die älter sind.

Der Befehl gibt eine Meldung mit dem Hinweis zurück, dass TruncateLog erfolgreich abgeschlossen wurde oder dass TruncateLog fehlgeschlagen ist. Der Kürzungsvorgang kann aus folgenden Gründen fehlschlagen:

- Der Ordnername ist ungültig.
- Der Arbeitsablauf ist im angegebenen Ordner nicht vorhanden.
- Sie haben zwar einen Arbeitsablauf angegeben, aber keinen Ordnernamen.

Der TruncateLog-Befehl verwendet die folgende Syntax:

```
truncatelog
-t <logs_truncated (all or up to end time in MM/DD/YYYY HH24:MI:SS format or as number
of days before current date)>
[-f <folder_name>]
[-w <workflow_name>]
```

In der folgenden Tabelle werden die Optionen und Argumente für `pmrep TruncateLog` beschrieben:

Option	Argument	Beschreibung
-t	logs_truncated	Erforderlich. Verwenden Sie „all“ zum Löschen aller Protokolle oder geben Sie einen Endzeitpunkt ein. <i>pmrep</i> löscht alle Protokolle, die nach dem Endzeitpunkt liegen. Sie können den Endzeitpunkt im Format MM/DD/YYYY HH24:MI:SS eingeben. Es ist aber auch möglich, die Anzahl der Tage vor dem aktuellen Datum anzugeben. Wenn Sie die Anzahl der Tage angeben, muss der Endzeitpunkt eine Ganzzahl größer als 0 sein.
-f	folder_name	Optional. Löscht mit dem Ordner verbundene Protokolle. Wenn Sie weder den Ordernamen noch den Arbeitsablaufnamen angeben, löscht <i>pmrep</i> alle Protokolle aus dem Repository.
-w	workflow_name	Optional. Löscht mit dem Arbeitsablauf verbundene Protokolle. Der Repository-Dienst löscht alle Protokolle aus dem Repository, wenn Sie nicht sowohl den Ordernamen als auch den Arbeitsablaufnamen angeben. Wenn Sie sowohl den Ordernamen als auch den Arbeitsablaufnamen angeben, löscht der Repository-Dienst mit dem Arbeitsablauf verbundene Protokolle. Wenn Sie den Arbeitsablaufnamen eingeben, müssen Sie auch den Ordernamen bereitstellen.

## UndoCheckout

Macht den Checkout eines Objekts rückgängig. Wenn Sie einen Checkout rückgängig machen, löst das Repository die Schreibprioritätssperre für das Objekt und kehrt zur zuletzt eing检ekten Version des Objekts zurück. Wenn Sie das Objekt wieder ändern möchten, müssen Sie es auschecken.

Der UndoCheckout-Befehl verwendet die folgende Syntax:

```
undocheckout
-o <object_type>
[-t <object_subtype>]
-n <object_name>
-f <folder_name>
[-s dbd_separator]
```

In der folgenden Tabelle werden die *pmrep* UndoCheckout-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	object_type	Erforderlich. Typ des Objekts. Sie können Quelle und Target, Transformation, Mapping, Sitzung, Worklet, Arbeitsablauf, Scheduler, Sitzungskonfiguration, Aufgabe, Cube und Größenordnung festlegen.
-t	object_subtype	Optional. Typ der Transformation oder Aufgabe. Ignoriert bei anderen Objekttypen. Weitere Informationen zu gültigen Subtypen finden Sie unter <a href="#">"Listing Object Types" auf Seite 1494</a> .
-n	object_name	Erforderlich. Name des ausgecheckten Objekts.

Option	Argument	Beschreibung
-f	folder_name	Erforderlich. Name des Ordners, der das Objekt enthält.
-s	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name\source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.

## Unregister

Hebt die Registrierung eines lokalen Repository in einem verbundenen globalen Repository auf.

Um diesen Befehl zu verwenden, müssen Sie den Repository Service für das lokale Repository im exklusiven Modus ausführen. Sie können die Ausführung des Repository Service im exklusiven Modus im Administrator-Tool konfigurieren oder den Befehl *infacmd* UpdateRepositoryService verwenden.

Der Befehl gibt die Meldung zurück, dass die Registrierung erfolgreich aufgehoben wurde oder dass die Registrierung nicht aufgehoben werden konnte. Die Registrierung schlägt möglicherweise aus folgenden Gründen fehl:

- Der Repository Service für das lokale Repository wird nicht im exklusiven Modus ausgeführt.
- Der Repository Service konnte Informationen zum globalen Repository nicht initialisieren.
- Die Verbindung zum Repository Service wurde nicht hergestellt.

Der Unregister-Befehl verwendet die folgende Syntax:

```
unregister
-r <local_repository_name>
-n <local_repository_user_name>
[-s <local_repository_user_security_domain>]
[-x <local_repository_password> |
-X <repository_password_environment_variable>]
[-d <local_repository_domain_name> |
-h <local_repository_portal_host_name>
-o <local_repository_portal_port_number>]] (if local repository is in a different domain)
```

In der folgenden Tabelle werden die *pmrep* Unregister-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-r	local_repository_name	Erforderlich. Name des lokalen Repository, dessen Registrierung aufgehoben werden soll.
-n	local_repository_user_name	Erforderlich. Lokaler Benutzernamen.

Option	Argument	Beschreibung
-s	local_repository_user_ security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Die Standardeinstellung ist "Native".
-x	local_repository_password	Erforderlich, wenn Sie nicht die Option -X verwenden. Anmelde-Passwort für das lokale Target-Repository. Sie müssen die Option -x oder -X verwenden, aber nicht beide.
-X	local_repository_password_ environment_variable	Erforderlich, wenn Sie nicht die Option -x verwenden. Anmelde-Passwort-Umgebungsvariable für das lokale Target-Repository. Sie müssen die Option -x oder -X verwenden, aber nicht beide.
-d	local_repository_domain_ name	Erforderlich, wenn sich das lokale Repository in einer anderen Domäne befindet und Sie nicht die Optionen -h und -o verwenden. Name der Informatica-Domäne für das Repository.
-h	local_repository_portal_host_ name	Erforderlich, wenn sich das lokale Repository in einer anderen Domäne befindet und Sie nicht die Option -d verwenden. Computername der Domäne, in der sich das lokale Repository befindet. Wenn Sie diese Option verwenden, müssen Sie auch die Option -o benutzen.
-o	local_repository_portal_port_ number	Erforderlich, wenn sich das lokale Repository in einer anderen Domäne befindet und Sie nicht die Option -d verwenden. Portnummer für die Domäne, in der sich das lokale Repository befindet. Wenn Sie diese Option verwenden, müssen Sie auch die Option -h verwenden.

## UnregisterPlugin

Entfernt ein Plug-In aus einem Repository. Sie können Plug-Ins hinzufügen und entfernen, um die Systemfunktionalität zu erweitern. Ein Plug-In ist ein Softwaremodul, das neue Repository-Metadaten einsetzt.

Wenn Sie diesen Befehl verwenden, muss der Repository Service im exklusiven Modus ausgeführt werden. Sie können die Ausführung des Repository Service im exklusiven Modus im Administrator-Tool konfigurieren oder den Befehl *infacmd UpdateRepositoryService* verwenden.

Der UnregisterPlugin-Befehl verwendet die folgende Syntax:

```
unregisterplugin
-v <vendor_id>
-l <plug-in_id>
[-s (is security module)
[-g (remove user-name-login mapping)]
{-w <new_password> |
-W <new_password_environment_variable>}]
```



In der folgenden Tabelle werden die *pmrep* UnregisterPlugin-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-v	vendor_id	Erforderlich. Kennzeichnet das Sicherheits-Plug-In anhand der Identifikationsnummer des Lieferanten. Sie definieren diese Zahl beim Registrieren des Plug-Ins.
-l	plug-in_id	Erforderlich. Kennzeichnet das Plug-In anhand der Identifikationsnummer. Sie definieren diese Identifikationsnummer beim Registrieren des Plug-Ins.
-s	-	Optional. Gibt an, ob das Modul ein externes Sicherheitsmodul ist.
-g	-	Optional. Beim Registrieren eines externen Sicherheitsmoduls anwendbar.  Entfernt die Zuordnung zwischen Benutzernamen und Anmeldennamen im Repository, wenn Sie die Registrierung eines externen Sicherheitsmoduls aufheben. Wenn Sie diese Option nicht angeben, bleibt die Zuordnung im Repository erhalten, aber der Repository Manager zeigt es nirgends an.  Verwenden Sie diese Option, wenn Sie die Registrierung eines Sicherheitsmoduls aufheben.
-w	new_password	Erforderlich, wenn das Plug-In ein Sicherheitsmodul enthält.  Erforderlich, wenn Sie nicht die Option -W verwenden. Sie müssen die Option -w oder -W verwenden, aber nicht beide.  Gibt ein neues Passwort für den Benutzer an, der den UnregisterPlugin-Befehl ausführt. Wenn Sie die Registrierung eines externen Authentifizierungsmoduls aufheben, werden alle Benutzerpasswörter auf die Werte im Repository zurückgesetzt. Sie müssen ein neues Passwort für den Zugriff auf das Repository eingeben.
-W	new_password_environment_variable	Erforderlich, wenn das Plug-In ein Sicherheitsmodul enthält.  Erforderlich, wenn Sie nicht die Option -w verwenden. Sie müssen die Option -w oder -W verwenden, aber nicht beide.  Gibt eine neue Passwortumgebungsvariable für den Benutzer an, der den Befehl zum Aufheben der Registrierung ausführt. Wenn Sie die Registrierung eines externen Authentifizierungsmoduls aufheben, werden alle Benutzerpasswörter auf die Werte im Repository zurückgesetzt. Sie müssen ein neues Passwort für den Zugriff auf das Repository eingeben.

## Aufheben der Registrierung eines externen Sicherheitsmoduls

Verwenden Sie den UnregisterPlugin-Befehl, um ein externes Sicherheitsmodul nicht mehr mit einem Repository zu verwenden. Wenn Sie die Registrierung des externen Sicherheitsmoduls aufheben, wechselt PowerCenter in den Repository-Authentifizierungsmodus. Alle Benutzerpasswörter werden auf die Werte im Repository und nicht auf die Werte im externen Verzeichnis zurückgesetzt. Wenn Sie die Registrierung des Sicherheitsmoduls aufheben, gehen die Mappings zwischen den Benutzernamen und den externen Sicherheitsanmeldennamen nicht verloren, sofern Sie nicht die Option -g eingeben. Verwenden Sie das Mapping erneut, wenn Sie ein neues Sicherheitsmodul registrieren.

**Hinweis:** Obwohl Sie die Zuordnungen zwischen externen Anmeldungen und Benutzernamen speichern können, zeigt der Repository Manager die externen Anmeldungen während der Ausführung unter der Benutzerauthentifizierung nicht an.

Sie müssen mithilfe der Option -w oder -W ein neues Passwort erstellen, wenn Sie die Registrierung des Sicherheitsmoduls aufheben.

## Beispiel

Als Administrator entscheiden Sie, aus dem LDAP-Sicherheitsmodul zurück zur Repository-Authentifizierung zu wechseln. Sie entfernen das Mapping zwischen Benutzername und Anmeldung. Alle Benutzer, die Sie unter der Repository-Authentifizierung zum System hinzugefügt haben, können sich mit ihren alten Benutzernamen und Passwörtern anmelden. Alle Benutzer, die Sie unter der LDAP-Sicherheit zum Repository hinzugefügt haben, können sich erst anmelden, wenn Sie die zugehörigen Benutzernamen aktivieren.

**Hinweis:** Sie müssen die LDAP-NIS-Anmeldung und das Passwort bereitstellen, um den Befehl `UnregisterPlugin` zu verwenden. Sie müssen außerdem ein neues Passwort bereitstellen, das Sie nach dem Wechsel zur Benutzerauthentifizierung verwenden können.

## UpdateConnection

Aktualisiert Benutzernamen, Passwort, Verbindungsstring und Attribute für eine Datenbankverbindung.

Der Befehl gibt die Meldung zurück, dass die Operation erfolgreich abgeschlossen wurde oder dass die Operation fehlgeschlagen ist. Ein Fehler kann aus den folgenden Gründen auftreten:

- Der Datenbanktyp wird nicht unterstützt.
- Das Verbindungsobjekt existiert nicht.
- *pmrep* kann keine Sperre für das Objekt abrufen.
- Einer der erforderlichen Parameter fehlt.

Der `UpdateConnection`-Befehl verwendet die folgende Syntax:

```
updateconnection
-t <connection_subtype>
-d <connection_name>
[[-u <new_user_name>]
[{-p <new_password> |
-P <new_password_environment_variable>
[-w (use parameter in password) |
-x (do not use parameter in password)}}] |
-K <connection_to_the_Kerberos_server>]
[-c <new_connection_string>]
[-a <attribute_name>
-v <new_attribute_value>]
[-s <connection type application, relational, ftp, loader or queue > ]
[-l <code page>]
[-S <odbc_subtype> (valid for ODBC connection only, default is None)]
```

In der folgenden Tabelle werden die *pmrep* UpdateConnection-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-t	connection_subtype	<p>Erforderlich. Zeigt den Verbindungsuntertyp an.</p> <p>Bei einer relationalen Verbindung gehören zu den Verbindungsuntertypen beispielsweise Oracle, Sybase und Microsoft SQL Server. Der gültige Subtyp für FTP-Verbindungen ist FTP.</p> <p>Eine Liste der vordefinierten Verbindungsuntertypen finden Sie unter <a href="#">"Verbindungsuntertypen" auf Seite 1445</a>.</p> <p><b>Hinweis:</b> Der Verbindungsuntertyp in der Option -t muss für den mit der Option -s angegebenen zugeordneten Verbindungstyp gültig sein.</p>
-d	connection_name	Erforderlich. Datenbankverbindungsname.
-u	new_user_name	Optional. Benutzername für die Authentifizierung, wenn Sie eine Verbindung zu der relationalen Datenbank herstellen.
-p	new_password	<p>Optional. Passwort für die Authentifizierung beim Herstellen einer Verbindung zur relationalen Datenbank. Verwenden Sie die Option -p oder -P, aber nicht beide.</p> <p>Um im Passwort einen Parameter anzugeben, fügen Sie das Präfix „\$Param“ für die Option -p hinzu, und stellen Sie sicher, dass Sie die Option -w verwenden. Verwenden Sie das Dollarzeichen (\$) ausschließlich in der Option -p und geben Sie das Parameterpasswort ohne Leerzeichen ein. Beispiel: -p '\$Param_abc' -w</p>
-P	new_password_environment_variable	Optional. Passwort-Umgebungsvariable für die Authentifizierung, wenn Sie eine Verbindung zu der relationalen Datenbank herstellen. Verwenden Sie die Option -p oder -P, aber nicht beide.
-w	-	<p>Optional. Ermöglicht es Ihnen, einen Parameter in der Passwortoption zu verwenden. <i>pmrep</i> verwendet das mit der Option -p oder -P angegebene Passwort als Namen des Sitzungsparameters zur Laufzeit.</p> <p>Nur gültig, wenn Sie die Option -p oder -P verwenden.</p> <p>Wenn Sie in der Passwortoption keinen Parameter festlegen, verwendet <i>pmrep</i> das mit der Option -p oder -P angegebene Benutzerpasswort.</p>
-x	-	<p>Optional. Deaktiviert die Verwendung von Passwortparametern, wenn Sie den Parameter im Passwort verwenden.</p> <p><i>pmrep</i> verwendet das mit der Option -p oder -P angegebene Passwort.</p>
-K	-	Optional. Gibt an, dass die Datenbank, zu der Sie eine Verbindung herstellen, in einem Netzwerk ausgeführt wird, das die Kerberos-Authentifizierung verwendet.
-c	new_connection_string	Optional. Verbindungszeichenfolge, die der Integrationsdienst verwendet, um eine Verbindung zur relationalen Datenbank herzustellen.
-a	attribute_name	Optional. Name des Attributs.
-v	new_attribute_value	Erforderlich, wenn Sie die Option -a verwenden. Neuer Attributwert der Verbindung. Geben Sie „Yes“ zum Aktivieren neuer Attribute und „No“ zum Deaktivieren neuer Attribute ein.

Option	Argument	Beschreibung
-s	Verbindungstypanwendung, relational, FTP, Loader oder Warteschlange	Optional. Typ der Verbindung. Folgende Verbindungstypen sind möglich: <ul style="list-style-type: none"> <li>- Anwendung</li> <li>- FTP</li> <li>- Loader</li> <li>- Warteschlange</li> <li>- Relational</li> </ul> Standardwert ist „relational“. <b>Hinweis:</b> Der Verbindungsuntertyp in der Option -t muss für den mit der Option -s angegebenen zugeordneten Verbindungstyp gültig sein.
-l	Codepage	Optional. Codepage, die der Verbindung zugeordnet ist.
-S	odbc_subtype	Optional. Aktiviert den ODBC-Untertyp für eine ODBC-Verbindung. Eine ODBC-Verbindung kann einen der folgenden ODBC-Untertypen aufweisen: <ul style="list-style-type: none"> <li>- AWS Redshift</li> <li>- Azure DW</li> <li>- Greenplum</li> <li>- Google Big Query</li> <li>- PostgreSQL</li> <li>- Snowflake</li> <li>- SAP HANA</li> <li>- Kein</li> </ul> Standardwert ist „Kein“.

Weitere Informationen über Verbindungsuntertypen finden Sie unter [“Verbindungsuntertypen” auf Seite 1445](#).

## UpdateEmailAddr

Aktualisiert mit den der Sitzung zugewiesenen E-Mail-Aufgaben verbundene E-Mail-Adressen für die Sitzungsbenachrichtigung. Wenn Sie zuvor keine Erfolgs- bzw. Fehler-E-Mail-Aufgabe für die Sitzung eingegeben haben, aktualisiert der Befehl die E-Mail-Adressen nicht. Sie können die E-Mail-Benachrichtigungsadressen für eine nicht wiederverwendbare Sitzung mit einem einmaligen Namen im Ordner aktualisieren. Sie können unterschiedliche Adressen für den Empfang von Erfolgs- oder Fehlerbenachrichtigungen eingeben. Dieser Befehl erfordert eine Verbindung zu einem Repository.

Der UpdateEmailAddr-Befehl verwendet die folgende Syntax:

```
updateemailaddr
-d <folder_name>
-s <session_name>
-u <success_email_address>
-f <failure_email_address>
```

In der folgenden Tabelle werden die *pmrep* UpdateEmailAddr-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-d	folder_name	Erforderlich. Name des Sitzungsordners.
-s	session_name	Erforderlich. Name der Sitzung.
-u	success_email_address	Erforderlich. E-Mail-Adresse zum Senden von Benachrichtigungen für erfolgreiche Sitzungen.
-f	failure_email_address	Erforderlich. E-Mail-Adresse zum Senden von Benachrichtigungen für fehlgeschlagene Sitzungen.

## UpdateSeqGenVals

Aktualisiert eine oder mehrere der folgenden Eigenschaften für die angegebene Sequenzgenerator-Transformation:

- Startwert
- Endwert
- Inkrementieren um
- Aktueller Wert

Möglicherweise möchten Sie Sequenzwerte beim Verschieben eines Mappings von einem Entwicklungsumfeld in eine Produktionsumgebung aktualisieren. Verwenden Sie den UpdateSeqGenVals-Befehl zum Aktualisieren wiederverwendbarer und nicht wiederverwendbarer Sequenzgenerator-Transformationen. Werte für Instanzen wiederverwendbarer Sequenzgenerator-Transformationen oder Shortcuts zu Sequenzgenerator-Transformationen können Sie jedoch nicht aktualisieren.

Der UpdateSeqGenVals-Befehl verwendet die folgende Syntax:

```
updateseqgenvals
-f <folder_name>
[-m <mapping_name>]
-t <sequence_generator_name>
[-s <start_value>]
[-e <end_value>]
[-i <increment_by>]
[-c <current_value>]
```

In der folgenden Tabelle werden die *pmrep* UpdateSeqGenVals-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-f	folder_name	Erforderlich. Ordnername.
-m	mapping_name	Mapping-Name. Beim Aktualisieren von Werten für eine nicht wiederverwendbare Sequenzgenerator-Transformation müssen Sie den Mapping-Namen einbeziehen.
-t	sequence_generator_name	Erforderlich. Sequenzgenerator-Transformationsname.
-s	start_value	Optional. Startwert der generierten Sequenz, die der Integration Service verwenden soll, wenn die Sequenzgenerator-Transformation die Zykluseigenschaft verwendet. Wenn Sie in den Transformationseigenschaften Zyklus auswählen, kehrt der Integration Service zu diesem Wert zurück, wenn er den Endwert erreicht.  Wenn Sie einen ungültigen Wert bestimmen, gibt <i>pmrep</i> eine Fehlermeldung aus und aktualisiert die Sequenzgenerator-Transformation nicht.
-e	end_value	Optional. Maximaler von Integration Service generierter Wert. Wenn der Integration Service diesen Wert während der Sitzung erreicht und die Sequenz nicht für den Zyklus konfiguriert ist, schlägt die Sitzung fehl.  Wenn Sie einen ungültigen Wert bestimmen, zeigt <i>pmrep</i> eine Fehlermeldung an und aktualisiert die Sequenzgenerator-Transformation nicht.
-i	increment_by	Optional. Unterschied zwischen zwei aufeinander folgenden Werten aus dem NEXTVAL-Port.  Wenn Sie einen ungültigen Wert bestimmen, zeigt <i>pmrep</i> eine Fehlermeldung an und aktualisiert die Sequenzgenerator-Transformation nicht.
-c	current_value	Optional. Aktueller Wert der Sequenz. Geben Sie den Wert ein, den der Integration Service als ersten Wert in der Sequenz verwenden soll. Wenn Sie eine Reihe von Werten nacheinander verwenden möchten, muss der aktuelle Wert größer oder gleich dem Anfangswert und kleiner als der Endwert sein.  Wenn Sie einen ungültigen Wert bestimmen, gibt <i>pmrep</i> eine Fehlermeldung aus und aktualisiert die Sequenzgenerator-Transformation nicht.

## UpdateSrcPrefix

Aktualisiert den Eigentümernamen für Sitzungsquelltabellen. Sie können den Eigentümernamen für eine oder alle Quellen in einer Sitzung aktualisieren. Updatesrcprefix aktualisiert den Eigentümernamen für Quelltabellen auf Sitzungsebene.

*pmrep* aktualisiert Eigentümernamen für Quelltabellen, wenn Sie zuvor den Quelltabellennamen in den Sitzungseigenschaften bearbeitet haben.

Der UpdateSrcPrefix-Befehl verwendet die folgende Syntax:

```
updatesrcprefix
-f <folder_name>
-s [<qualifying_path>.]<session_name>
[-t <source_name>]
-p <prefix_name>
[-n (use source instance name; not using -n gives old, deprecated behavior)]
```

In der folgenden Tabelle werden die *pmrep* UpdateSrcPrefix-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-f	folder_name	Erforderlich. Name des Ordners, der die Sitzung enthält.
-s	session_name	Erforderlich. Name der Sitzung, in der die zu aktualisierenden Quellen enthalten sind. Geben Sie für wiederverwendbare Sitzungen den Sitzungsnamen ein. Für nicht wiederverwendbare Sitzungen müssen Sie außerdem den Sitzungspfad eingeben, z. B. <i>worklet_name.session_name</i> oder <i>workflow_name.session_name</i> .
-t	source_name	Optional. Name der zu aktualisierenden Quelle. Wenn Sie diese Option nicht angeben, aktualisiert <i>pmrep</i> alle Eigentümernamen für Quelltabellen in der Sitzung. Wenn Sie die Option -n einbeziehen, können Sie den Namen der Quellinstanz wie in den Sitzungseigenschaften angezeigt oder als Ausgabe des ListTablesBySess-Befehls eingeben. Obwohl der UpdateSrcPrefix-Befehl auch ohne die Option -n ausgeführt wird, beziehen Sie die Option -n ein, um den Quellinstanznamen zu verwenden. Wenn Sie die Option -n nicht angeben, müssen Sie den DBD-Namen und die Quelltabellenamen als <i>dbd_name.source_name</i> eingeben. Der Quell-DBD-Name befindet sich im Designer Navigator. Der Designer generiert den DBD-Namen aus dem Quelltyp oder Datenquellnamen beim Erstellen einer Quelldefinition im Repository.
-p	prefix_name	Erforderlich. Eigentümernamen, den Sie in der Quelltable aktualisieren möchten.
-n	-	Optional. Gleicht das source_name-Argument mit Quellinstanznamen ab. Obwohl der UpdateSrcPrefix-Befehl auch ohne die Option -n ausgeführt wird, beziehen Sie die Option -n ein, um den Quellinstanznamen zu verwenden. Wenn Sie diese Option nicht angeben, gleicht <i>pmrep</i> das source_name-Argument mit den Quelltabellenamen ab.

## UpdateStatistics

Aktualisiert die Statistiken für Repository-Tabellen und -Indizes.

Der Befehl gibt „updatestatistics erfolgreich abgeschlossen“ oder „updatestatistics fehlgeschlagen“ zurück.

Der UpdateStatistics-Befehl verwendet die folgende Syntax:

```
updatestatistics
```

## UpdateTargPrefix

Aktualisiert den Tabellennamenspräfix für Sitzungs-Target-Tabellen. Der Tabellennamenspräfix gibt den Eigentümer der Tabelle in der Datenbank an. Sie können den Eigentümernamen eines oder aller in einer Sitzung angegebenen Targets aktualisieren. UpdateTargPrefix aktualisiert den Namenspräfix der Target-Tabelle auf Sitzungsebene.

*pmrep* aktualisiert Tabellennamenspräfixe, wenn Sie zuvor den Tabellennamenspräfix auf Sitzungsebene bearbeitet haben.

Der UpdateTargPrefix-Befehl verwendet die folgende Syntax:

```
updatetargprefix
-f <folder_name>
-s [<qualifying_path>.]<session_name>
[-t <target_name>]
-p <prefix_name>

[-n (use target instance name; not using -n gives old, deprecated behavior)]
```

In der folgenden Tabelle werden die *pmrep* UpdateTargPrefix-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-f	folder_name	Erforderlich. Name des Ordners, der die Sitzung enthält.
-s	session_name	Erforderlich. Name der Sitzung, in der die zu aktualisierenden Ziele enthalten sind. Geben Sie für wiederverwendbare Sitzungen den Sitzungsnamen ein. Für nicht wiederverwendbare Sitzungen geben Sie den Sitzungsnamen und -pfad ein, z. B. <i>worklet_name.session_name</i> oder <i>workflow_name.session_name</i> .
-t	target_name	Optional. Name des zu aktualisierenden Ziels. Wenn Sie diese Option nicht angeben, aktualisiert <i>pmrep</i> alle Namenspräfixe von Zieltabellen in der Sitzung. Wenn Sie die Option -n einbeziehen, können Sie den Namen der Zielinstanz wie in den Sitzungseigenschaften angezeigt oder als Ausgabe des ListTablesBySess-Befehls eingeben. Obwohl der UpdateTargPrefix-Befehl auch ohne die Option -n ausgeführt wird, beziehen Sie die Option -n ein, um den Zielinstanznamen zu verwenden. Wenn Sie die Option -n nicht angeben, müssen Sie den Zieltabellennamen anstelle des Zielinstanznamens eingeben.



Option	Argument	Beschreibung
-p	prefix_name	Erforderlich. Tabellennamenspräfix, das Sie in der Zieltabelle aktualisieren möchten.
-n	-	Optional. Gleicht das Zielnamensargument mit den Zielinstanznamen ab. Obwohl der UpdateTargPrefix-Befehl auch ohne die Option -n ausgeführt wird, beziehen Sie die Option -n ein, um den Zielinstanznamen zu verwenden. Wenn Sie diese Option nicht angeben, gleicht <i>pmrep</i> das Zielnamensargument mit den Zieltabellennamen ab.

## Upgrade

Aktualisiert ein Repository auf die neueste Version.

Der Upgrade-Befehl verwendet die folgende Syntax:

```
upgrade
[-x <repository_password_for_confirmation> |
-X <repository_password_environment_variable_for_confirmation>]
```

In der folgenden Tabelle werden *pmrep* Upgrade-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-x	repository_password_for_confirmation	Optional. Passwort. Sie können die Option -x oder -X Option verwenden, aber nicht beide. Wenn Sie weder die Option -x noch -X verwenden, werden Sie von <i>pmrep</i> aufgefordert, zur Bestätigung das Passwort einzugeben.
-X	repository_password_environment_variable_for_confirmation	Erforderlich, wenn Sie nicht die Option -x verwenden. Passwort-Umgebungsvariable. Sie müssen die Option -x oder -X verwenden, aber nicht beide.

## UninstallAbapProgram

Deinstalliert das ABAP-Programm. Deinstallieren Sie ein ABAP-Programm, wenn das Programm nicht länger einem Mapping zugeordnet werden soll. Der Befehl deinstalliert die Programme vom SAP-System und entfernt die entsprechenden Programminformationen aus dem PowerCenter Repository.

Der UninstallAbapProgram-Befehl verwendet die folgende Syntax:

```
uninstallabaprogram
-s <folder_name>
-m <mapping_name>
```

```

[-v <version_number>]

[-l <log_filename>]

-u <user_name>

-x <password>

-c <connect_string>

-t <client>

[-y <language>]

-p <program_mode (file, stream)>

```

In der folgenden Tabelle werden die pmrep UninstallAbapProgram-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-s	folder_name	Erforderlich. Der Name des Ordners, in dem das Mapping des ABAP-Programms enthalten ist, das Sie deinstallieren möchten.
-m	mapping_name	Erforderlich. Name des Mappings.
-v	version_number	Optional. Versionsnummer des Mappings. Standardmäßig ist die neueste Version.
-l	log_filename	Optional. Name der Protokolldatei, in die der Befehl die Informationen oder Fehlermeldungen schreibt. Standardmäßig wird die Protokolldatei in dem Verzeichnis gespeichert, in dem Sie den Befehl ausführen.
-u	user_name	Erforderlich. Benutzername für die SAP-Quellsystemverbindung. Muss ein Benutzer sein, für den Sie eine Quellsystemverbindung erstellt haben.
-x	passwort	Erforderlich. Passwort für den Benutzernamen. Verwenden Sie das Befehlszeilenprogramm pmpasswd zum Verschlüsseln des Benutzerpassworts.
-c	connect_string	Erforderlich. In der Datei <code>sapnwrfc.ini</code> definierter DEST-Eintrag für eine Verbindung mit einem bestimmten SAP-Anwendungsserver oder für eine Verbindung, die den SAP-Lastenausgleich verwendet.
-t	Client	Erforderlich. SAP-Clientnummer.
-y	Sprache	Optional. SAP-Anmeldesprache. Muss mit der Codepage des PowerCenter Client kompatibel sein. Standardwert ist die Sprache des SAP-Systems.
-p	program_mode (file, stream)	Erforderlich. Modus, in denen der PowerCenter-Integrationsdienst Daten aus dem SAP-System extrahiert. Wählen Sie die Datei oder den Stream aus.

## Beispiel

Das folgende Beispiel deinstalliert das ABAP-Programm:

```

uninstallabaprogram -s folder_name -m mapping_name -l logfile_name -u user_name -x
password -c connect_string -t 800 -y EN -p stream

```

# Validieren

Validiert Objekte. Sie können die Ergebnisse in eine persistente Ausgabedatei oder Standardausgabe ausgeben.

Es zeigt außerdem eine Zusammenfassung der Validierung in „stdout“ an. Die Zusammenfassung enthält die Anzahl der gültigen Objekte, ungültigen Objekte und übersprungenen Objekte. Die persistente Ausgabedatei enthält Standardinformationen, kodierte IDs und eine CRC-Überprüfung. Sie können die Objekte speichern und einchecken, die von ungültig zu gültig wechseln.

Sie können die folgenden Objekttypen validieren:

- Zuordnungen
- Mapplets
- Sitzungen
- Arbeitsabläufe
- Worklet-Objekte

Wenn Sie im Eingabeparameter einen anderen Objekttyp verwenden, gibt *pmrep* einen Fehler zurück. Wenn Sie in einer persistenten Eingabedatei den falschen Objekttyp verwenden, berichtet *pmrep* einen Fehler und überspringt das Objekt.

**Hinweis:** Der *pmrep* Validate-Befehl validiert keine Shortcuts.

Wenn Sie Validate ausführen, können Sie Informationen zum Objektstatus ausgeben:

- **valid.** Objekte wurden erfolgreich validiert.
- **saved.** Objekte wurden nach der Validierung gespeichert.
- **skipped.** Shortcuts und Objekttypen, die keine Validierung erfordern.
- **save\_failed.** Objekte, die aufgrund von Sperrkonflikten nicht gespeichert wurden oder von einem anderen Benutzer ausgecheckt wurden.
- **invalid\_before.** Objekte, die vor der Validierungsprüfung ungültig sind.
- **invalid\_after.** Objekte, die nach der Validierungsprüfung ungültig sind.

Ein nicht wiederverwendbares Objekt kann erst gespeichert werden, wenn das wiederverwendbare übergeordnete Objekt des Objekts gespeichert wird. Wenn Sie die Option *-s* verwenden, speichert der Befehl keine validierten nicht wiederverwendbaren Objekte, es sei denn, Sie listen als Teil desselben Befehls wiederverwendbare Objekte auf, die als übergeordnete Objekte der nicht wiederverwendbaren Objekte fungieren.

Der Validate-Befehl verwendet die folgende Syntax:

```
validate
{{-n <object_name>
-o <object_type (mapplet, mapping, session, worklet, workflow)>
[-v <version_number>]
[-f <folder_name>]} |
-i <persistent_input_file>}
[-s (save upon valid)
[-k (check in upon valid)
[-m <check_in_comments>]]]
[-p <output_option_types (valid, saved, skipped, save_failed, invalid_before,
invalid_after, or all)>]
[-u <persistent_output_file_name>
[-a (append)]]
[-c <column_separator>]
[-r <end-of-record_separator>]
[-l <end-of-listing_indicator>]
```

```
[-b (verbose)]
[-y (print database type)]
```

In der folgenden Tabelle werden die Optionen und Argumente für „*pmrep Validate*“ beschrieben:

Option	Argument	Beschreibung
-n	object_name	Erforderlich. Name des zu validierenden Objekts. Verwenden Sie diese Option nicht bei Verwendung des Arguments -i. Schließen Sie beim Validieren einer nicht wiederverwendbaren Sitzung den Namen des Arbeitsablaufs ein. Geben Sie den Namen des Arbeitsablaufs und den Namen der Sitzung in folgendem Format ein: <Name des Arbeitsablaufs>.<Name der Sitzungsinstanz> Wenn Sie eine nicht wiederverwendbare Sitzung in einem nicht wiederverwendbaren Worklet validieren, geben Sie den Namen des Arbeitsablaufs, des Worklets und der Sitzung in folgendem Format ein: <Name des Arbeitsablaufs>.<worklet name>.<Name der Sitzungsinstanz>
-o	object_type	Erforderlich, wenn Sie keine persistente Eingabedatei verwenden. Zu validierender Objekttyp. Sie können Mapplets, Zuordnungen, Sitzungen, Worklets und Arbeitsabläufe angeben.
-v	version_number	Optional. Version des zu validierenden Objekts. Standardwert ist die neueste oder ausgecheckte Version des Objekts.
-f	folder_name	Erforderlich. Name des Ordners, der das Objekt enthält.
-i	persistent_input_file	Optional. Textdatei aus dem Befehl ExecuteQuery, Validate oder ListObjectDependencies. Enthält eine Liste mit Objektdatensätzen. Sie können diese Datei nicht verwenden, wenn Sie Objekte mithilfe der Argumente -n, -o oder -f angeben.
-s	-	Optional. Speichern Sie Objekte, die von ungültig zu gültig wechseln, im Repository.
-k	-	Erforderlich, wenn Sie -s verwenden. Checken Sie gespeicherte Objekte ein.
-m	check_in_comments	Erforderlich, wenn Sie die Option -k verwenden. Zudem erfordert das aktuelle Repository Eincheck-Kommentare. Fügen Sie beim Einchecken eines Objekts Kommentare hinzu.
-p	output_option_types	Erforderlich, wenn Sie das Argument -u verwenden. Objekttyp, den Sie nach der Validierung in die persistente Ausgabedatei oder in „stdout“ ausgeben möchten. Sie können valid, saved, skipped, save_failed, invalid_before oder invalid_after angeben. Geben Sie eine oder mehrere Optionen durch Kommas getrennt ein.
-u	persistent_output_file_name	Erforderlich, wenn Sie das Argument -p verwenden. Name einer Ausgabedatei. Wenn Sie einen Dateinamen eingeben, schreibt die Abfrage die Ergebnisse in eine Datei.
-a	append	Optional. Hängt die Ergebnisse an die persistente Ausgabedatei an, statt sie zu überschreiben.

Option	Argument	Beschreibung
-c	column_separator	Optional. Zeichen oder Zeichenfolgen zum Trennen von Spalten mit Objektmetadaten. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Wenn ein Repository-Objektnamen Leerzeichen enthält, sollten Sie kein Leerzeichen als Spaltentrennzeichen verwenden. Wenn Sie diese Option auslassen, verwendet <i>pmrep</i> ein einzelnes Leerzeichen.
-r	end-of-record_separator	Optional. Zeichen oder Zeichenfolgen, die das Ende der Objektmetadaten kennzeichnen. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Standardwert ist „newline“ /n.
-l	end-of-listing_indicator	Optional. Zeichen oder Zeichenfolgen, die das Ende der Objektliste kennzeichnen. Geben Sie ein Zeichen oder eine Zeichenfolge ein, die nicht in Repository-Objektnamen verwendet wird. Wenn Sie diese Option auslassen, verwendet <i>pmrep</i> einen Punkt.
-b	-	Optional. Verbose. Zeigt neben den Mindestinformationen weitere Informationen zu den Objekten an. Wenn Sie diese Option auslassen, zeigt <i>pmrep</i> ein reduziertes Format an, einschließlich des Objekttyps, wiederverwendbarer oder nicht wiederverwendbarer Wörter, des Objektnamens und -pfads. Verbose-Format enthält die Versionsnummer und den Ordernamen. Das Kurzformat für globale Objekte, wie Beschriftung, Abfrage, Bereitstellungsgruppe und Verbindung, enthält den Objekttyp und den Objektnamen. Verbose-Format enthält den Erstellernamen und den Zeitpunkt der Erstellung.
-y	-	Optional. Zeigt den Datenbanktyp von Quellen und Zielen an.

## Version

Zeigt die PowerCenter-Version und Informatica-Handelsmarke sowie Urheberrechtsinformationen an.

Der Version-Befehl verwendet die folgende Syntax:

```
version
```

# KAPITEL 45

## Arbeiten mit filemanager

Dieses Kapitel umfasst die folgenden Themen:

- [filemanager Overview, 1538](#)
- [copy, 1540](#)
- [copyfromlocal, 1541](#)
- [list, 1542](#)
- [move, 1543](#)
- [remove, 1545](#)
- [rename, 1546](#)
- [watch, 1547](#)

### filemanager Overview

The filemanager utility administers preprocessing and file-watching capabilities for a cloud ecosystem such as Amazon AWS or Microsoft Azure.

You can use the filemanager utility for the following preprocessing capabilities:

- List files on a cloud ecosystem.
- Copy files on a cloud ecosystem.
- Copy files from a local system to a cloud ecosystem.
- Move files on a cloud ecosystem.
- Rename files on a cloud ecosystem.
- Delete files from a cloud ecosystem.

You can use the filemanager utility for the following file-watching capabilities:

- Trigger a file-processing event.
- Trigger a workflow or mapping.

You can use the filemanager utility from one of the following locations:

- Client directory. Available under `<Infa home>/clients/tools/filemanager`
- Server directory. Available under `<Infa home>/tools/filemanager`

## Logging Options

The filemanager utility provides the following log severity levels for debugging purposes:

- FINE. Writes severe, info, and warning messages to the log. The fine or debug messages are user-request logs.
- SEVERE. Writes severe, warning, and error messages to the log. The severe messages include non-recoverable system failures, connection failures, and service errors.
- WARNING. Writes severe, warning, and error messages to the log. The warning errors include recoverable system failures and warnings.
- INFO. Writes severe, info, warning, and error messages to the log. The info messages include system and service change messages.

## Default Behavior

The filemanager utility exhibits the following default behavior:

- The filemanager utility treats \ as an escape character and not a separator in cloud paths.
- The filemanager utility creates a target directory if you do not specify a target directory for move, copy, or rename operations in Amazon AWS cloud ecosystem.
- The filemanager utility creates a target directory if you do not specify a target directory for a copy operation in ADLS Gen2 storage. For other file operations, the filemanager utility displays an error.
- The filemanager utility deletes the target directory if you move or rename a file to a target directory that does not exist and then try to move the file back to the source directory.
- The filemanager utility displays a file name in the logs when you move, copy, rename, or remove a file.
- The filemanager utility does not display a file name in the logs when you remove a file stored in ADLS Gen2 storage.
- The list command does not specify whether a listed object is a file or a folder.
- The watch command triggers the mapping before a file gets copied in Microsoft Azure cloud ecosystem. This action applies to ADLS Gen1 storage and when you use external tools to copy a file.
- The copy and list commands do not work if you specify a folder path in the parameter `-bn<-bucketname>`.

## Guidelines

Use the following guidelines when you use the filemanager utility:

- You must have connection, read, and execute permissions to run the filewatcher utility.
- You cannot copy an empty folder.
- Do not use multiple / to specify cloud paths.
- Do not use a file path in a pattern search.
- Do not use a symbolic link that points to the same directory recursively.
- Set the environment variables INFA\_TRUSTSTORE and INFA\_TRUSTSTORE\_PASSWORD if the domain is enabled with a custom SSL.
- Set the environment variable INFA\_TRUSTSTORE if the domain is SSL enabled.
- Set the first three parameters in a command as: `filemanager <cloud ecosystem> <command>`. For example, `filemanager aws list`
- Use the absolute path for file names.

- Use the parameter `-dn<domainname|optional>` for multiple domains configured in Informatica Administrator.
- When you use the watch command, place the parameter `-op<other parameters|optional>` at the end of the syntax.
- Use only the following wildcard characters to specify patterns:
  - .
  - ?
  - ""
  - \*

## copy

Verwenden Sie den Befehl „copy“, um Dateien in ein Amazon AWS-Cloud-Ökosystem zu kopieren.

Der Befehl `copy` von `filemanager` verwendet die folgende Syntax:

```
copy
[<-bucketname|-bn> bucket_name]
<-old_filename|-fn> old_filename
<-new_foldername|-nfn> new_foldername
<-new_bucketname|-nbn> new_bucketname
<-username|-un> user_name
<-password|-pd> password
[<-security_domainname|-sdn> security_domain]
<-connection|-cn> connection
[<-domainname|-dn> domain_name]
```

In der folgenden Tabelle werden die Optionen für den Befehl „copy“ von `filemanager` beschrieben:

Option	Beschreibung
<code>-bucketname</code> <code>-bn</code>	Optional. Der Name des Buckets, der Dateien enthält.
<code>-old filename</code> <code>-fn</code>	Der Name der Quelldatei oder des Ordners, den Sie kopieren möchten.
<code>-new_foldername</code> <code>-nfn</code>	Der Name des Zielordners, in den Sie die Dateien kopieren möchten.
<code>-new_bucketname</code> <code>-nbn</code>	Der Name des Buckets, in den Sie die Dateien kopieren möchten.



Option	Beschreibung
Benutzername -un	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne.
-password -pd	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet.
security_domainname -sdn	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Beim Namen der Sicherheitsdomäne wird zwischen Groß- und Kleinschreibung unterschieden. Wenn für die Domäne die native oder LDAP-Authentifizierung verwendet wird, ist „Nativ“ der Standardwert. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
Verbindung -cn	Name der Verbindung im Informatica Administrator.
-DomainName -dn	Optional. Name der Informatica-Domäne. Nur erforderlich, wenn im Informatica Administrator mehrere Domänen konfiguriert sind.

## copyfromlocal

Verwenden Sie den Befehl `copyfromlocal` zum Kopieren von Dateien aus einem lokalen System in ein Cloud-Ökosystem.

Der Befehl `copyfromlocal` von `filemanager` verwendet die folgende Syntax:

```
copyfromlocal
[<-bucketname|-bn> bucket_name]
[<-cloudpath|-cp> cloud_path]
<-localpath|-lp> local_path
<-username|-un> user_name
<-password|-pd> password
[<-security_domainname|-sdn> security_domain]
<-connection|-cn> connection
[<-folderpath|-fp> folder_path]
[<-domainname|-dn> domain_name]
```

In der folgenden Tabelle werden die Optionen für den Befehl copyfromlocal von filemanager beschrieben:

Option	Beschreibung
-bucketname -bn	Optional. Der Name des Buckets, der Dateien oder den Ordner enthält. Diese Option gilt für Amazon AWS.
-cloudpath -cp	Pfad zu den Cloud-Dateien, in den Sie kopieren möchten. Diese Option gilt für Microsoft Azure.
-localpath -lp	Pfad zu den Quelldateien oder zum Ordner auf einem lokalen System, die Sie kopieren möchten.
Benutzername -un	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne.
-password -pd	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet.
security_domainname -sdn	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
Verbindung -cn	Name der Verbindung im Informatica Administrator.
-FolderPath -fp	Optional. Pfad zu den Dateien in der Cloud, in den Sie kopieren möchten. Diese Option gilt für Amazon AWS.
-DomainName -dn	Optional. Name der Informatica-Domäne. Nur erforderlich, wenn im Informatica Administrator mehrere Domänen konfiguriert sind.

## list

Verwenden Sie den Befehl list zum Auflisten von Dateien in einem Cloud-Ökosystem.

Der filemanager-Befehl list verwendet die folgende Syntax:

```
list  
  
[<-bucketname|-bn> bucket_name]  
  
[<-cloudpath|-cp> cloud_path]  
  
<-pattern|-ptn> pattern  
  
<-username|-un> user_name  
  
<-password|-pd> password  
  
[<-security_domainname|-sdn> security_domain]
```

```

<-connection|-cn> connection

<-folderpath|-fp> folder_path

[<-domainname|-dn> domain_name]

```

In der folgenden Tabelle werden die Optionen für den filemanager-Befehl list beschrieben:

Option	Beschreibung
-bucketname -bn	Optional. Der Name des Buckets, der Dateien enthält. Diese Option gilt für Amazon AWS.
-cloudpath -cp	Pfad zu den Cloud-Dateien, in den Sie kopieren möchten. Diese Option gilt für Microsoft Azure.
-pattern -ptn	Ein Platzhaltermuster zum Abgleichen und Auflisten von Dateinamen oder Mustern.
-username -un	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne.
-password -pd	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet.
security_domainname -sdn	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Beim Namen der Sicherheitsdomäne wird zwischen Groß- und Kleinschreibung unterschieden. Wenn für die Domäne die native oder LDAP-Authentifizierung verwendet wird, ist „Nativ“ der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-connection -cn	Name der Verbindung im Informatica Administrator.
-folderpath -fp	Optional. Pfad zum Auflisten der Dateien in der Cloud. Diese Option gilt für Amazon AWS.
-domainname -dn	Optional. Name der Informatica-Domäne. Nur erforderlich, wenn im Informatica Administrator mehrere Domänen konfiguriert sind.

## move

Verwenden Sie den Befehl move zum Verschieben von Dateien in einem Cloud-Ökosystem.

Im Microsoft Azure-Cloud-Ökosystem unterstützt der Befehl move den Verschiebevorgang nicht, wenn das Zielverzeichnis nicht vorhanden ist.

Der filemanager-Befehl move verwendet die folgende Syntax:

```

move

[<-bucketname|-bn> bucket_name]

```

```

<source_cloudpath|-scp> source_cloudpath

<destination_cloudpath|-dcp> destination_cloudpath

<-old_filename|-fn> old_filename]

<-new_folder|-nfn> new_folder]

<-new_bucketname|-nbn> new_bucketname

<-username|-un> user_name

<-password|-pd> password

[<-security_domainname|-sdn> security_domain]

<-connection|-cn> connection

[<-domainname|-dn> domain_name]

```

In der folgenden Tabelle werden die Optionen für den filemanager-Befehl move beschrieben:

Option	Beschreibung
-bucketname -bn	Optional. Der Name des Buckets, der Dateien enthält. Diese Option gilt für Amazon AWS.
-old_filename -fn	Pfad des Quelldateinamens, von dem aus Sie die Datei verschieben möchten. Diese Option gilt für Amazon AWS.
-new_folder -nfn	Pfad zum Speicherort des Zielordners, an den Sie die Datei verschieben möchten. Diese Option gilt für Amazon AWS.
-new_bucketname -nbn	Pfad zum Zielbucket, an den Sie die Datei verschieben möchten. Diese Option gilt für Amazon AWS.
-source_cloudpath -scp	Pfad des Speicherorts der Quelldatei im Microsoft Azure Cloud-Ökosystem, von dem aus Sie die Datei verschieben möchten. Diese Option gilt für Microsoft Azure.
-destination_cloudpath -dcp	Pfad zum Speicherort des Zielordners im Microsoft Azure Cloud-Ökosystem, an den Sie die Datei verschieben möchten. Diese Option gilt für Microsoft Azure.
Benutzername -un	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne.
-password -pd	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet.
security_domainname -sdn	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Beim Namen der Sicherheitsdomäne wird zwischen Groß- und Kleinschreibung unterschieden. Wenn für die Domäne die native oder LDAP-Authentifizierung verwendet wird, ist „Nativ“ der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Beschreibung
Verbindung -cn	Name der Verbindung im Informatica Administrator.
-DomainName -dn	Optional. Name der Informatica-Domäne. Nur erforderlich, wenn im Informatica Administrator mehrere Domänen konfiguriert sind.

## remove

Verwenden Sie den Befehl `remove` zum Löschen von Dateien aus einem Cloud-Ökosystem.

Der `filemanager`-Befehl `remove` verwendet die folgende Syntax:

```
remove
[<-bucketname|-bn> bucket_name]
<cloudpath|-cp> source_cloudpath
<-filename|-fn> old_filename]
<-username|-un> user_name
<-password|-pd> password
[<-security_domainname|-sdn> security_domain]
<-connection|-cn> connection
<-folderpath|-fp> folder_path
[<-domainname|-dn> domain_name]
```

In der folgenden Tabelle werden die Optionen für den `filemanager`-Befehl `remove` beschrieben:

Option	Beschreibung
-bucketname -bn	Optional. Der Name des Buckets, der Dateien enthält. Diese Option gilt für Amazon AWS.
-filename -fn	Der Name der Datei oder des Ordners, den Sie löschen möchten. Diese Option gilt für Amazon AWS.
-cloudpath -cp	Pfad zur Datei oder zum Ordner im Microsoft Azure Cloud-Ökosystem, aus dem Sie die Datei löschen möchten. Diese Option gilt für Microsoft Azure.
Benutzername -un	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne.
-password -pd	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet.

Option	Beschreibung
security_domainname -sdn	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Beim Namen der Sicherheitsdomäne wird zwischen Groß- und Kleinschreibung unterschieden. Wenn für die Domäne die native oder LDAP-Authentifizierung verwendet wird, ist „Nativ“ der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
Verbindung -cn	Name der Verbindung im Informatica Administrator.
-FolderPath -fp	Optional. Pfad zu den Dateien in der Cloud, aus dem Sie die Datei löschen möchten. Diese Option gilt für Amazon AWS.
-DomainName -dn	Optional. Name der Informatica-Domäne. Nur erforderlich, wenn im Informatica Administrator mehrere Domänen konfiguriert sind.

## rename

Verwenden Sie den Befehl `rename` zum Umbenennen von Dateien in einem Cloud-Ökosystem.

Der `filemanager`-Befehl `rename` verwendet die folgende Syntax:

```

rename
[<-bucketname|-bn> bucket_name]
<-old_filename|-fn> old_filename
<-new_filename|-nfn> new_filename
[<-cloudpath|-cp> cloud_path]
<-username|-un> user_name
<-password|-pd> password
[<-security_domainname|-sdn> security_domainname]
<-connection|-cn> connection
[<-domainname|-dn> domain_name]
```

In der folgenden Tabelle werden die Optionen für den `filemanager`-Befehl `rename` beschrieben:

Option	Beschreibung
-bucketname -bn	Optional. Der Name des Buckets, der Dateien enthält. Diese Option gilt für Amazon AWS.
-old filename -fn	Pfad zur Quelldatei oder zum alten Dateinamen, den Sie umbenennen möchten. Diese Option gilt für Amazon AWS.

Option	Beschreibung
-new_filename -nfn	Pfad zur Zielfeile oder zum neuen Dateinamen.
-cloudpath -cp	Pfad zur Cloud-Datei, von dem aus Sie die Datei umbenennen möchten. Diese Option gilt für Microsoft Azure.
Benutzername -un	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne.
-password -pd	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet.
security_domainname -sdn	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Beim Namen der Sicherheitsdomäne wird zwischen Groß- und Kleinschreibung unterschieden. Wenn für die Domäne die native oder LDAP-Authentifizierung verwendet wird, ist „Nativ“ der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
Verbindung -cn	Name der Verbindung im Informatica Administrator.
-DomainName -dn	Optional. Name der Informatica-Domäne. Nur erforderlich, wenn im Informatica Administrator mehrere Domänen konfiguriert sind.

## watch

Verwenden Sie den Befehl watch zum Überwachen von Dateien, die ein Dateiverarbeitungsereignis, eine Zuordnung oder einen Arbeitsablauf in einem Cloud-Ökosystem auslösen.

Der filemanager-Befehl watch verwendet die folgende Syntax:

```

watch
[<-bucketname|-bn> bucket_name]
[<-cloudpath|-cp> cloud_path]
<-pattern|-ptn> pattern
<-username|-un> user_name
<-password|-pd> password
[<-security_domainname|-sdn> security_domainname]
<-connection|-cn> connection
<-Domainname|-dn> domain_name of the DIS
<-DIS|-sn> Data Integration Service
<-applicationname|-a> application_name

```

```

<-mappingname|-m> mapping_name

<-workflowname|-w> workflow_name

[<-watchtime|-wt> watch_time]

[<-folderpath|-fp> folder_path

[<-other_parameters|-op> custom_infacmd_mapping_parameters

```

In der folgenden Tabelle werden die Optionen für den filemanager-Befehl watch beschrieben:

Option	Beschreibung
-bucketname -bn	Optional. Der Name des Buckets, der Dateien oder den Ordner enthält. Diese Option gilt für Amazon AWS.
-cloudpath -cp	Pfad zu den Cloud-Dateien, die Sie überwachen möchten. Diese Option gilt für Microsoft Azure.
Muster -ptn	Ein Platzhaltermuster zum Abgleichen und Auflisten von Dateinamen oder Mustern.
Benutzername -un	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne.
-password -pd	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet.
security_domainname -sdn	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Beim Namen der Sicherheitsdomäne wird zwischen Groß- und Kleinschreibung unterschieden. Wenn für die Domäne die native oder LDAP-Authentifizierung verwendet wird, ist „Nativ“ der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
Verbindung -cn	Name der Verbindung im Informatica Administrator.
-Domainname -dn	Erforderlich. Name der Domäne, die den Datenintegrationsdienst ausführt.
-DIS -sn	Name des Datenintegrationsdiensts, der einer Zuordnung oder einen Arbeitsablauf ausführt.
-applicationname -a	Name der Anwendung, die einen Arbeitsablauf oder eine Zuordnung enthält.
-mappingname -m	Erforderlich, wenn Sie eine Zuordnung überwachen möchten. Name der Zuordnung, die Sie überwachen möchten.
-workflowname -w	Erforderlich, wenn Sie einen Arbeitsablauf überwachen möchten. Name des Arbeitsablaufs, den Sie überwachen möchten.



Option	Beschreibung
-watchtime -wt	Optional. Die Dauer in Minuten, um die Datei zu überwachen.
-FolderPath -fp	Optional. Pfad zu den Dateien in der Cloud, in den Sie kopieren möchten. Diese Option gilt für Amazon AWS.
-other_parameters -op	Optional. Benutzerdefinierte Parameter, die Sie im Dienstprogramm infacmd verwenden möchten.

## KAPITEL 46

# Arbeiten mit pmrep-Dateien

Dieses Kapitel umfasst die folgenden Themen:

- [Arbeiten mit pmrep-Dateien - Übersicht, 1550](#)
- [Verwenden der persistenten Eingabedatei , 1550](#)
- [Verwenden der Objektimport-Steuerdatei, 1553](#)
- [Objektimport-Steuerdatei – Beispiele, 1557](#)
- [Verwenden der Bereitstellungssteuerdatei , 1564](#)
- [Bereitstellungs-Steuerdatei – Beispiele, 1571](#)
- [Tipps für die Arbeit mit pmrep-Dateien, 1572](#)

## Arbeiten mit pmrep-Dateien - Übersicht

*pmrep* enthält eine Reihe von Steuerdateien, mit denen Sie definieren können, wie Objekte ins Repository importiert werden. Die Steuerdateiparameter verwenden dieselben Parameter in der Steuerdatei, die Sie im PowerCenter Client verwenden. Sie können die folgenden Steuerdateien verwenden:

- **Persistente Eingabedatei.** Verwenden Sie eine persistente Eingabedatei, um Repository-Objekte anzugeben, die Sie verarbeiten möchten.
- **Objektimport-Steuerdatei.** Verwenden Sie die Objektimport-Steuerdatei und geben Sie eine Reihe von Fragen an, um zu definieren, wie Objekte importiert werden.
- **Bereitstellungssteuerdatei** Sie können die Objekte in einer dynamischen oder statischen Bereitstellungsgruppe in mehrere Target-Ordner im Target-Repository kopieren.

## Verwenden der persistenten Eingabedatei

Wenn Sie *pmrep* mit einigen Aufgaben ausführen, verwenden Sie eine persistente Eingabedatei zum Angeben der Repository-Objekte, die Sie verarbeiten möchten. Die persistente Eingabedatei repräsentiert bereits im Repository vorhandene Objekte. Sie können eine persistente Eingabedatei manuell oder mithilfe von *pmrep* erstellen.

Verwenden Sie eine persistente Eingabedatei mit den folgenden *pmrep*-Befehlen:

- **AddToDeploymentGroup.** Fügt Objekte einer Bereitstellungsgruppe hinzu.
- **ApplyLabel.** Beschriftet Objekte.

- **ExecuteQuery.** Führt eine Abfrage aus, um eine persistente Eingabedatei zu erstellen. Verwenden Sie die Datei für andere *pmrep*-Befehle.
- **ListObjectDependencies.** Listet Abhängigkeitsobjekte auf. Dieser Befehl kann eine persistente Eingabedatei für die Verarbeitung verwenden und er kann eine erstellen.
- **MassUpdate.** Aktualisiert die Sitzungseigenschaften für eine Reihe von Sitzungen.
- **ObjectExport.** Exportiert Objekte in eine XML-Datei.
- **Validate.** Validiert Objekte. Dieser Befehl kann eine persistente Eingabedatei für die Verarbeitung verwenden und er kann eine erstellen.

Die persistente Eingabedatei verwendet das folgende Format:

```
encoded ID, foldername, object_name, object_type, object_subtype, version_number,
reusable|non-reusable
```

## Erstellen einer persistenten Eingabedatei mit pmrep

Sie können eine persistente Eingabedatei unter Verwendung der *pmrep*-Befehle *ExecuteQuery*, *Validate* oder *ListObjectDependencies* erstellen. Mithilfe dieser Befehle werden Dateien erstellt, die eine Liste von Objekten mit verschlüsselten IDs und einem CRC-Wert (Cyclic Redundancy Check, zyklische Redundanzprüfung) enthalten. Weiterhin ist eine verschlüsselte Repository-GID enthalten. Mit dieser ID wird das Repository angegeben, aus dem der Datensatz stammt.

Die *pmrep*-Befehle, die eine persistente Eingabedatei verwenden, rufen die Objektinformationen aus den verschlüsselten IDs ab. Die verschlüsselten IDs ermöglichen *pmrep* die schnelle Verarbeitung der Eingabedatei.

Beim Erstellen einer persistenten Eingabedatei mit *pmrep* wird diese im *pmrep*-Installationsverzeichnis gespeichert. Sie können einen anderen Pfad angeben.

Der folgende Text zeigt ein Beispiel für eine persistente Eingabedatei:

```
2072670638:57bfc2ff-df64-40fc-9cd4-
a15cb489bab8:3538944199885:138608640183285:1376256153425:131072168215:65536142655:0288235
:088154:65536122855,EXPORT,M_ITEMS,mapping,none,2
1995857227:57bfc2ff-df64-40fc-9cd4-
a15cb489bab8:3538944135065:13867417666804:1376256233835:19660880104:65536271545:0319425:0
17154:6553644164,EXPORT,M_ITEMS_2,mapping,none,3
1828891977:57bfc2ff-df64-40fc-9cd4-
a15cb489bab8:3538944279765:138739712184505:137625613474:65536221345:65536133675:091734:09
053:65536156675,EXPORT,M_NIELSEN,mapping,none,1
3267622055:57bfc2ff-df64-40fc-9cd4-
a15cb489bab8:353894462954:138805248300075:1376256151365:6553675414:65536174015:0273455:02
41435:65536261685,EXPORT,M_OS1,mapping,none,1
```

## Beispiel

Sie können den Befehl *ExecuteQuery* zum Erstellen einer persistenten Eingabedatei für Objekte verwenden, die in einem anderen *pmrep*-Befehl verarbeitet werden. Sie möchten beispielsweise alle logisch gelöschten Objekte aus dem Repository exportieren. Sie können eine Abfrage mit der Bezeichnung "find\_deleted\_objects" erstellen. Wenn Sie die Abfrage wie hier angezeigt mit *pmrep* ausführen, werden alle gelöschten Objekte im Repository gefunden und die Ergebnisse in eine persistente Eingabedatei geschrieben:

```
ExecuteQuery -q find_deleted_objects -t private -u deletes_workfile
```

Sie können "deletes\_workfile" dann als persistente Eingabedatei für *ObjectExport* verwenden:

```
ObjectExport -i deletes_workfile -u exported_del_file
```

*ObjectExport* exportiert alle referenzierten Objekte in eine XML-Datei mit der Bezeichnung "exported\_del\_file".

## Manuelles Erstellen einer persistenten Eingabedatei

Wenn Sie *pmrep*-Befehle für eine Gruppe von Objekten ausführen möchten, die über Befehle wie *ExecuteQuery* nicht ermittelt werden können, besteht die Möglichkeit zur manuellen Erstellung einer Eingabedatei.

Verwenden Sie die folgenden Regeln und Richtlinien, wenn Sie eine persistente Eingabedatei erstellen:

- Geben Sie "none" für die verschlüsselte ID ein. Die *pmrep*-Befehle erhalten die Objektinformationen aus den anderen Argumenten in den Datensätzen.
- Geben Sie für Quellobjekte den Objektnamen wie folgt ein: <DBD\_name>.<source\_name>.
- Geben Sie für Objekte, wie z. B. Mappings, die nicht über *sub\_type* verfügen, "none" als *object\_subtype* ein oder nehmen Sie keine Eingabe vor. Weitere Informationen zu gültigen Umwandlungen und Aufgabentypen finden Sie unter ["Listing Object Types" auf Seite 1494](#).
- Geben Sie bei versionierten Repositories die Versionsnummer des gewünschten Objekts ein. Alternativ können Sie auch "AKTUELL" eingeben, um die aktuelle Version des Objekts zu verwenden.
- Lassen Sie bei unversionierten Repositories das Argument *version\_number* leer.
- Ignorieren Sie das Argument bei Objekttypen, wie z. B. Targets, die weder wiederverwendbar noch nicht wiederverwendbar sein können.
- Nicht wiederverwendbare Objekte können nicht aufgenommen werden. Sie können das wiederverwendbare übergeordnete Objekt des nicht wiederverwendbaren Objekts angeben.

Sie möchten beispielsweise die Objektabhängigkeiten für eine nicht wiederverwendbare Filtertransformation auflisten. Sie können das Mapping, das als übergeordnetes Objekt der Transformation fungiert, angeben:

```
none,CAPO,m_seqgen_map,mapping,none,1,reusable
```

Das Mapping *m\_seqgen\_map* ist das wiederverwendbare übergeordnete Objekt der Filtertransformation. Der Befehl wird erfolgreich ausgeführt, wenn Sie das wiederverwendbare übergeordnete Objekt angeben.

**Hinweis:** Wenn Sie eine manuell erstellte persistente Eingabedatei verwenden, gibt der Repository Service eine Meldung mit dem Hinweis zurück, dass die ID ungültig ist. Hierbei handelt es sich um eine Informationsmeldung. Der Repository Service erkennt, dass es sich um eine manuell erstellte Eingabedatei handelt, und kann den Befehl mit "none" als ID verarbeiten.

### Beispiel

Das folgende Beispiel zeigt eine manuell erstellte persistente Eingabedatei:

```
none,EXPORT,CustTgt,target,none,2
none,EXPORT,S_Orders,session,,2,reusable
none,EXPORT,EXP_CalcTot,transformation,expression,LATEST,reusable
```

Im ersten Datensatz handelt es sich bei *CustTgt* um eine Target-Definition. Targets haben keinen Untertyp, d. h., Sie geben "none" für das Argument *object\_subtype* ein. Ein Target kann weder wiederverwendbar noch nicht wiederverwendbar sein, daher kann das Wiederverwendbarkeitsargument weggelassen werden. Beachten Sie, dass der Datensatz sechs statt sieben Argumente aufweist.

Im zweiten Datensatz handelt es sich bei *S\_Orders* um eine Sitzung. Sitzungen haben keinen Untertyp, d. h. Sie lassen das Argument leer.

Der dritte Datensatz soll die aktuelle Version der Transformation aufweisen, d. h., Sie geben "LATEST" für das Argument *version\_number* ein.

# Verwenden der Objektimport-Steuerdatei

Wenn Sie den *pmrep* ObjectImport-Befehl verwenden, können Sie mit einer Steuerdatei Fragen beantworten, die Sie in der Regel beim Importieren von Objekten mit dem Importassistenten bearbeiten. Zum Erstellen einer Steuerdatei müssen Sie eine durch *impcntl.dtd* definierte XML-Datei erstellen. Die Importsteuerdatei wird mit dem PowerCenter Client installiert. Sie müssen deren Speicherort in der Eingabe-XML-Datei aufnehmen.

Im Folgenden sehen Sie ein Beispiel für eine *impcntl.dtd*-Datei:

```
<!-- Informatica Object Import Control DTD Grammar - >

<!--IMPORTPARAMS This inputs the options and inputs required for import operation -->
<!--CHECKIN_AFTER_IMPORT Check in objects on successful import operation -->
<!--CHECKIN_COMMENTS Check in comments -->
<!--APPLY_LABEL_NAME Apply the given label name on imported objects -->
<!--RETAIN_GENERATED_VALUE Retain existing sequence generator, normalizer and XML DSQ
current values in the destination -->
<!--COPY_SAP_PROGRAM Copy SAP program information into the target repository -->
<!--APPLY_DEFAULT_CONNECTION Apply the default connection when a connection used by a
session does not exist in the target repository -->
<!ELEMENT IMPORTPARAMS (FOLDERMAP*, TYPEFILTER*, RESOLVECONFLICT?)>
<!--ATTLIST IMPORTPARAMS
      CHECKIN_AFTER_IMPORT          (YES | NO) "NO"
      CHECKIN_COMMENTS              CDATA      #IMPLIED
      APPLY_LABEL_NAME              CDATA      #IMPLIED
      RETAIN_GENERATED_VALUE        (YES | NO) "NO"
      COPY_SAP_PROGRAM              (YES | NO) "YES"
      APPLY_DEFAULT_CONNECTION      (YES | NO) "NO"
>

<!--FOLDERMAP matches the folders in the imported file with the folders in the target
repository -->
<!ELEMENT FOLDERMAP EMPTY>
<!--ATTLIST FOLDERMAP
      SOURCEFOLDERNAME              CDATA      #REQUIRED
      SOURCEREPOSITORYNAME          CDATA      #REQUIRED
      TARGETFOLDERNAME              CDATA      #REQUIRED
      TARGETREPOSITORYNAME          CDATA      #REQUIRED
>

<!--Import will only import the objects in the selected types in TYPEFILTER node -->
<!--TYPENAME type name to import. This should conforming to the element name in
powermart.dtd, e.g. SOURCE, TARGET and etc.-->
<!ELEMENT TYPEFILTER EMPTY>
<!--ATTLIST TYPEFILTER
      TYPENAME                      CDATA      #REQUIRED
>

<!--RESOLVECONFLICT allows to specify resolution for conflicting objects during import.
The combination of specified child nodes can be supplied -->
<!ELEMENT RESOLVECONFLICT (LABELOBJECT | QUERYOBJECT | TYPEOBJECT | SPECIFICOBJECT)*>

<!--LABELOBJECT allows objects in the target with label name to apply replace/reuse upon
conflict -->
<!ELEMENT LABELOBJECT EMPTY>
<!--ATTLIST LABELOBJECT
      LABELNAME                     CDATA      #REQUIRED
      RESOLUTION                    (REPLACE | REUSE | RENAME) #REQUIRED
>

<!--QUERYOBJECT allows objects result from a query to apply replace/reuse upon conflict
-->
<!ELEMENT QUERYOBJECT EMPTY>
<!--ATTLIST QUERYOBJECT
      QUERYNAME                     CDATA      #REQUIRED
      RESOLUTION                    (REPLACE | REUSE | RENAME) #REQUIRED
>
```

```

<!--TYPEOBJECT allows objects of certain type to apply replace/reuse upon conflict-->
<!ELEMENT TYPEOBJECT EMPTY>
<!ATTLIST TYPEOBJECT
OBJECTTYPENAME          CDATA          #REQUIRED
RESOLUTION              REPLACE | REUSE | RENAME)  #REQUIRED
>

<!--SPECIFICOBJECT allows a particular object(name, typename etc.) to apply replace/
reuse upon conflict -->
<!--NAME Object name-->
<!--EXTRNAME Source DBD name - required for source object to identify uniquely-->
<!--OBJECTTYPENAME Object type name-->
<!--FOLDERNAME Folder which the object belongs to-->
<!--REPOSITORYNAME Repository name that this object belongs to-->
<!--RESOLUTION Resolution to apply for the object in case of conflict-->
<!ELEMENT SPECIFICOBJECT EMPTY>
<!ATTLIST SPECIFICOBJECT
NAME                    CDATA          #REQUIRED
DBDNAME                CDATA          #IMPLIED
OBJECTTYPENAME         CDATA          #REQUIRED
FOLDERNAME             CDATA          #REQUIRED
REPOSITORYNAME         CDATA          #REQUIRED
RESOLUTION              REPLACE | REUSE | RENAME)  #REQUIRED
>

```

## Objektimport-Steuerdatei-Parameter

In der folgenden Tabelle finden Sie eine Auflistung der *pmrep*-Objektimport-Steuerdatei-Parameter:

Element	Attributname	Attributbeschreibung
IMPORTPARAMS	CHECKIN_AFTER_IMPORT	Bei Aktivierung der Versionsverwaltung erforderlich. Checkt Objekte nach erfolgreichem Import ein.
IMPORTPARAMS	CHECKIN_COMMENTS	Optional. Wendet die Kommentare auf die eingetragenen Objekte an.
IMPORTPARAMS	APPLY_LABEL_NAME	Optional. Wendet die Beschriftung auf die importierten Objekte an.
IMPORTPARAMS	RETAIN_GENERATED_VALUE	Bei Verwendung von Sequenzgenerator-, Normalisierungsprogramm- oder XML-Quellqualifikator-Transformationen erforderlich. Behält vorhandene Werte der Sequenzgenerator-, Normalisierungsprogramm- oder XML-Quellqualifikator-Transformationen im Ziel bei.
IMPORTPARAMS	COPY_SAP_PROGRAM	Optional. Kopiert SAP-Programminformationen in das Target-Repository.

Element	Attributname	Attributbeschreibung
IMPORTPARAMS	APPLY_DEFAULT_CONNECTION	Optional. Wendet die Standardverbindung an, wenn eine von einer Sitzung verwendete Verbindung im Target-Repository nicht vorhanden ist. Die Standardverbindung ist die erste Verbindung aus der sortierten Liste der verfügbaren Verbindungen. Sucht die Liste der Verbindungen im Workflow Manager.
FOLDERMAP	SOURCEFOLDERNAME	Erforderlich. Importiert den Ordernamen in Übereinstimmung mit einem Ordner im Target-Repository.
FOLDERMAP	SOURCEREPOSITORYNAME	Erforderlich. Repository mit dem Quellordner.
FOLDERMAP	TARGETFOLDERNAME	Erforderlich. Target-Ordnername für Matching.
FOLDERMAP	TARGETREPOSITORYNAME	Erforderlich. Repository mit dem Target-Ordner.
TYPEFILTER	TYPENAME	Optional. Importiert die Objekte aus einem bestimmten Knoten, z. B. Quellen, Targets oder Mappings.
RESOLVECONFLICT	LABELOBJECT-, QUERYOBJECT-, TYPEOBJECT- UND SPECIFICOBJECT-Elemente.	Sie können Konfliktlösungen für Objekte angeben.
LABELOBJECT	LABELNAME	Erforderlich. Kennzeichnet Objekte nach Beschriftungsname für die Konfliktlösungsspezifikation.
LABELOBJECT	RESOLUTION	Erforderlich. Ersetzen, wiederverwenden, umbenennen.
QUERYOBJECT	QUERYNAME	Erforderlich. Kennzeichnet Objekte aus dieser Abfrage für die Konfliktlösungsspezifikation.
QUERYOBJECT	RESOLUTION	Erforderlich. Ersetzen, wiederverwenden oder umbenennen.
TYPEOBJECT	OBJECTTYPENAME	Erforderlich. Objekttyp für diese Konfliktlösung. Eine Liste mit Objekttypen finden Sie unter <a href="#">"Objektimport-Steuerdatei-Parameter" auf Seite 1554</a> .
TYPEOBJECT	RESOLUTION	Erforderlich. Ersetzen, wiederverwenden oder umbenennen.

Element	Attributname	Attributbeschreibung
SPECIFICOBJECT	NAME	Erforderlich. Spezifischer Objektname für diese Konfliktlösung.
SPECIFICOBJECT	DBDNAME	Optional. Quell-DBD zum Identifizieren des Quellobjekts.
SPECIFICOBJECT	OBJECTTYPE	Erforderlich. Objekttyp für diese Konfliktlösung. Eine Liste mit Objekttypen finden Sie unter <a href="#">"Objektimport-Steuerdatei-Parameter" auf Seite 1554</a> .
SPECIFICOBJECT	FOLDERNAME	Erforderlich. Quellordner, der das Objekt enthält.
SPECIFICOBJECT	REPOSITORYNAME	Erforderlich. Quell-Repository, in dem das Objekt enthalten ist.
SPECIFICOBJECT	RESOLUTION	Erforderlich. Ersetzen, wiederverwenden oder umbenennen.

Sie können folgende Objekttypen mit dem OBJECTTYPE-Attribut verwenden:

- Alle
- Aggregator
- Anwendungs-Mehrfachgruppen-Quellqualifikator
- Anwendungsquellenqualifikator
- Zuweisung
- Befehl
- Kontrolle
- Benutzerdefinierte Umwandlung
- Entscheidung
- E-Mail
- Event-Raise
- Event-Wait
- Ausdruck
- Externe Prozedur
- Filter
- Eingabeumwandlung
- Joiner
- Lookup-Verfahren
- Mapping
- Mapplet
- MQ-Quellqualifikator



- Normalizer
- Ausgabeumwandlung
- Rang
- Router
- Scheduler
- Sitzung
- Sequenz
- SessionConfig
- Sortierer
- Quelldefinition
- Quellqualifikator
- Start
- Zieldefinition
- Timer
- Transaktionssteuerung
- Update-Strategie
- Benutzerdefinierte Funktion
- Arbeitsablauf
- Worklet
- XML-Quellqualifikator

**Hinweis:** Verwenden Sie den Objekttyp "Alle", um alle Objekte wiederzuverwenden oder zu ersetzen.

## Objektimport-Steuerdatei – Beispiele

Die im Code der Steuerdatei von Ihnen angegebenen Parameter bestimmen die Aktionen, die beim Ausführen des Befehls `ObjectImport` in *pmrep* durchgeführt werden. In den folgenden Beispielen werden Instanzen beschrieben, in denen der Befehl `ObjectImport` zusammen mit einer Steuerdatei zum Importieren von Repository-Objekten verwendet wird. Die Elemente und Attributnamen, die für die Durchführung der beschriebenen Aufgaben benötigt werden, sind im Code mit Kommentaren gekennzeichnet.

In der folgenden Tabelle werden Beispiele für Objektimport-Steuerdateien beschrieben:

Funktion	Beschreibung
Importieren von Quellobjekten.	Verwenden des Elements <code>TYPEFILTER</code> , um ausschließlich Quellobjekte zu importieren.
Importieren mehrerer Objekte in einen Ordner.	Verwenden der Elemente <code>IMPORTPARAMS</code> und <code>FOLDERMAP</code> , um mehrere Objekte zu importieren.
Einchecken und Beschriften importierter Objekte.	Verwenden der Attribute <code>CHECKIN_AFTER_IMPORT</code> und <code>APPLY_LABEL_NAME</code> des Elements <code>IMPORTPARAMS</code> , um importierte Objekte zu beschriften.

Funktion	Beschreibung
Beibehalten von Werten für Sequenzgenerator- und Normalisierungsprogramm-Transformationen.	Verwenden des Attributs RETAIN_GENERATED_VALUE des Elements IMPORTPARAMS, um Sequenzgenerator- und Normalisierungsprogramm-Werte beim Import von Objekten beizubehalten.
Importieren von Objekten und lokalen Shortcut-Objekten in dasselbe Repository.	Verwenden aller Attribute des Elements FOLDERMAP zum Importieren von Objekten und lokalen Shortcut-Objekten, die auf die Objekte verweisen.
Importieren von Shortcut-Objekten aus einem anderen Repository.	Verwenden aller Attribute des Elements FOLDERMAP, um Shortcut-Objekte aus einem anderen Repository zu importieren.
Importieren von Objekten in mehrere Ordner.	Verwenden aller Attribute des Elements FOLDERMAP zum Importieren von Objekten in mehrere Ordner.
Importieren bestimmter Objekte.	Verwenden des Elements TYPEFILTER zum Importieren bestimmter Objekte.
Erneutes Verwenden und Ersetzen abhängiger Objekte.	Verwenden der Attribute OBJECTTYPENAME und RESOLUTION des Elements TYPEOBJECT, um abhängige Objekte erneut zu verwenden und zu ersetzen.
Ersetzen ungültiger Mappings.	Verwenden des Elements QUERYOBJECT, um ungültige Mappings zu ersetzen.
Umbenennen von Objekten.	Verwenden des Attributs RESOLUTION des Elements SPECIFICOBJECT, um Objekte umzubenennen.
Kopieren von SAP-Mappings und SAP-Programminformationen.	Verwenden des Attributs COPY_SAP_PROGRAM des Elements IMPORTPARAMS, um SAP-Mappings und SAP-Programminformationen zu kopieren.
Anwenden von Standard-Verbindungsattributen.	Verwenden des Attributs APPLY_DEFAULT_CONNECTION des Elements IMPORTPARAMS, um standardmäßige Verbindungsattribute anzuwenden.
Lösen von Objektkonflikten.	Verwenden des Elements RESOLVECONFLICT, um Objektkonflikte zu lösen.

## Importieren von Quellobjekten

Quellobjekte können importiert werden. Sie möchten beispielsweise alle doppelten Objekte mit der Bezeichnung "Monatsende" im Zielordner ersetzen. Sie möchten jedoch kollidierende Quellobjekte, die "Jahr\_Ende" im Objektnamen enthalten, umbenennen. Sie verfügen über eine Abfrage mit der Bezeichnung "Jahr\_ENDE\_Abfrage", die diese Objekte findet.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="NO">
<FOLDERMAP SOURCEFOLDERNAME="OLD_ACCOUNTING"
  SOURCEREPOSITORYNAME="OLD_REPOS"
  TARGETFOLDERNAME="NEW_ACCOUNTING"
  TARGETREPOSITORYNAME="NEW_REPOS"/>

<!-- use the TYPEFILTER element to import only source objects -->
<TYPEFILTER TYPENAME="SOURCE"/>
<RESOLVECONFLICT>
  <LABELOBJECT LABELNAME="Monthend">
```

```

    RESOLUTION = "REPLACE"/>
<QUERYOBJECT QUERYNAME ="yr_end_qry"
    RESOLUTION = "RENAME"/>
</RESOLVECONFLICT>
</IMPORTPARAMS>

```

## Importieren von mehreren Objekten in einen Ordner

Sie können mehrere Objekte in einen Ordner importieren, diese einchecken und beschriften. Sie möchten beispielsweise die Objekte in Ordner SRC\_F1 importieren und die Objekte mit LABEL\_IMPORT\_NEW beschriften.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```

<xml version="1.0" encoding="UTF-16LE"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<!--apply label name LABEL_IMPORT_NEW to imported objects-->
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="NEWOBJECTS"
  APPLY_LABEL_NAME="LABEL_IMPORT_NEW">
<FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="SRC_REPO1"
  TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="TGT_REPO1"/>
</IMPORTPARAMS>

```

## Einchecken der und Beschriften von importierten Objekten

Sie können Objekte in einen Ordner importieren, diese einchecken und beschriften sowie Konflikte zwischen Sitzungskonfigurationsobjekten lösen. Sie möchten beispielsweise die Objekte aus Ordner SRC\_F1 exportieren und in Ordner TGT\_F1 importieren. Der Repository Service erstellt standardmäßig eine Sitzungskonfiguration im Target-Ordner. Sie schließen das Attribut APPLY\_LABEL\_NAME in das Element IMPORTPARAMS ein, um die importierten Objekte zu beschriften, und das Element RESOLVECONFLICT in die Steuerdatei, um den Konflikt zu lösen.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```

<?xml version="1.0" encoding="UTF-16LE"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<!--enter VERSION1 as the comment for the object you check in-->
<!--apply label name LABEL_IMPORT_NEW to imported objects-->

<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="VERSION1"
  APPLY_LABEL_NAME="LABEL_IMPORT_NEW">
<FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="SRC_REPO1"
  TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="TGT_REPO1"/>
<RESOLVECONFLICT>
<TYPEOBJECT OBJECTTYPE="SessionConfig" RESOLUTION="REUSE"/>
</RESOLVECONFLICT>
</IMPORTPARAMS>

```

## Beibehalten von Sequenzgenerator- und Normalisierungsprogramm-Werten

Beim Importieren von Objekten und Ersetzen aller Objekte im Zielordner können Sie die Werte von Sequenzgenerator- und Normalisierungsprogramm-Transformationen beibehalten.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```

<?xml version="1.0" encoding="UTF-16LE"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<!--enter YES as the value for the RETAIN_GENERATED_VALUE attribute -->
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="VERSION1"
  APPLY_LABEL_NAME="LABEL_IMPORT_NEW" RETAIN_GENERATED_VALUE="YES">w

```

```
<FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="SRC_REPO1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="TGT_REPO1"/>
<RESOLVECONFLICT>
<TYPEOBJECT OBJECTTYPENAME="ALL" RESOLUTION="REPLACE"/>
</RESOLVECONFLICT>
</IMPORTPARAMS>
```

## Importieren von Objekten und lokalen Shortcut-Objekten zum selben Repository

Sie können Objekte und die zugehörigen lokalen Shortcut-Objekte in dasselbe Repository importieren. Sie verfügen beispielsweise über Ordner mit den Bezeichnungen SRC\_SHARED\_F1 und SRC\_NONSHARED\_F1. Der Ordner SRC\_NONSHARED\_F1 ist nicht freigegeben und enthält lokale Shortcut-Objekte, die auf Objekte im Ordner SRC\_SHARED\_F1 verweisen. Sie möchten die Objekte in verschiedene Ordner im Target-Repository importieren. Darüber hinaus sollen die Shortcut-Objekte im Ordner TGT\_NONSHARED\_F1 auf die Objekte im Ordner TGT\_SHARED\_F1 zeigen.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="NO">

<!-- import objects from SRC_SHARED_F1 to TGT_SHARED_F1, and shortcut objects from
SRC_NONSHARED_F1 to TGT_NONSHARED_F1-->
<FOLDERMAP SOURCEFOLDERNAME="SRC_SHARED_F1" SOURCEREPOSITORYNAME="SRC_REPO1"
TARGETFOLDERNAME="TGT_SHARED_F1" TARGETREPOSITORYNAME="TGT_REPO1"/>
<FOLDERMAP SOURCEFOLDERNAME="SRC_NONSHARED_F1" SOURCEREPOSITORYNAME="SRC_REPO1"
TARGETFOLDERNAME="TGT_NONSHARED_F1" TARGETREPOSITORYNAME="TGT_REPO1"/>
</IMPORTPARAMS>
```

## Importieren von Shortcut-Objekten aus einem anderen Repository

Sie können Objekte aus anderen Repositories importieren. Sie verfügen beispielsweise über Ordner in einem lokalen Repository, das Shortcuts zu Objekten in einem globalen Repository enthält. Sie möchten die globalen Shortcut-Objekte in ein Repository importieren, das im globalen Repository registriert ist, und Shortcuts zu den ursprünglichen Objekten im globalen Repository beibehalten.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="global objects"
APPLY_LABEL_NAME="LABEL_IMPORT_GLOBAL_SHORTCUT">

<!--import the shortcut objects from source folder SRC_SHARED_F1 in source repository
SRC_GDR_REPO1 to source folder SRC_SHARED_F1 in target repository SRC_GDR_REPO2 -->

<FOLDERMAP SOURCEFOLDERNAME="SRC_SHARED_F1" SOURCEREPOSITORYNAME="SRC_GDR_REPO1"
TARGETFOLDERNAME="SRC_SHARED_F1" TARGETREPOSITORYNAME="SRC_GDR_REPO2"/>
<FOLDERMAP SOURCEFOLDERNAME="SRC_NONSHARED_F1" SOURCEREPOSITORYNAME="SRC_LDR_REPO1"
TARGETFOLDERNAME="TGT_NONSHARED_F1" TARGETREPOSITORYNAME="SRC_LDR_REPO2"/>
</IMPORTPARAMS>
```

## Importieren von Objekten in mehrere Ordner

Sie können Objekte in mehrere Ordner importieren, die aus mehreren Ordnern exportiert wurden. Sie haben beispielsweise Objekte aus den Ordnern SRC\_F1, SRC\_F2 und SRC\_F3 exportiert und möchten sie in die Target-Ordner TGT\_F1, TGT\_F2, TGT\_F3 in Repository TGT\_REPO1 importieren.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="mulfolders"
APPLY_LABEL_NAME="L1">

  <!-- import objects from source folders SRC_F1, SRC_F2, and SRC_F3 to target folders
  TGT_F1, TGT_F2, and TGT_F3 in repository TGT_REPO1 -->
  <FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="SRC_REPO1"
  TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="TGT_REPO1"/>
  <FOLDERMAP SOURCEFOLDERNAME="SRC_F2" SOURCEREPOSITORYNAME="SRC_REPO2"
  TARGETFOLDERNAME="TGT_F2" TARGETREPOSITORYNAME="TGT_REPO1"/>
  <FOLDERMAP SOURCEFOLDERNAME="SRC_F3" SOURCEREPOSITORYNAME="SRC_REPO3"
  TARGETFOLDERNAME="TGT_F3" TARGETREPOSITORYNAME="TGT_REPO1"/>
  <RESOLVECONFLICT>
  <TYPEOBJECT OBJECTTYPE = "SESSIONCONFIG" RESOLUTION="REUSE"/>
</RESOLVECONFLICT>

</IMPORTPARAMS>
```

## Importieren von spezifischen Objekten

Sie können die Objekte auswählen, die Sie importieren möchten. Sie können beispielsweise mehrere Objekttypen in eine XML-Datei exportieren. Sie möchten nur Mappings und die jeweiligen Quellen und Targets in einen Ordner importieren.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="PMREP_IMPORT_TYPEFILTER"
APPLY_LABEL_NAME="LABEL MAPPING TYPEFILTER">
  <FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="REPO_EX_1"
  TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="REPO_EX1_"/>

  <!-- use the TYPENAME attribute to import only mappings -->
  <TYPEFILTER TYPENAME="MAPPING"/>
</IMPORTPARAMS>
```

## Wiederverwenden und Ersetzen von abhängigen Objekten

Sie können Sitzungen importieren, Mappings ersetzen und vorhandene Quellen und Targets im Target-Ordner wiederverwenden. Sie möchten beispielsweise die Mappings ersetzen und die Quelldefinitionen, Target-Definitionen und Sitzungskonfigurationsobjekte wiederverwenden.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">

<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="PMREP_IMPORT_TYPEFILTER"
APPLY_LABEL_NAME="LABEL_SESSION_TYPEFILTER">
  <FOLDERMAP SOURCEFOLDERNAME="PMREP_CHECKED_OUT" SOURCEREPOSITORYNAME="REPO_EX_1"
  TARGETFOLDERNAME="PMREP_CHECKED_OUT_IMPORT_TYPEFILTER_SESSION"
  TARGETREPOSITORYNAME="REPO_EX_1"/>
  <TYPEFILTER TYPENAME="SESSION"/>
  <RESOLVECONFLICT>

  <!-- replace all mappings -->
  <TYPEOBJECT OBJECTTYPE = "MAPPING" RESOLUTION="REPLACE"/>

  <!-- reuse source definitions, target definitions, and sessionconfigs -->
  <TYPEOBJECT OBJECTTYPE = "SOURCE DEFINITION" RESOLUTION="REUSE"/>
  <TYPEOBJECT OBJECTTYPE = "TARGET DEFINITION" RESOLUTION="REUSE"/>
```

```

<TYPEOBJECT OBJECTTYPENAME = "SESSIONCONFIG" RESOLUTION="REUSE"/>

<!-- replace some object types and reuse remaining objects-->
<TYPEOBJECT OBJECTTYPENAME = "ALL" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME = "SOURCE DEFINITION" RESOLUTION="REPLACE"/>
<TYPEOBJECT OBJECTTYPENAME = "MAPPING" RESOLUTION="REPLACE"/>

</RESOLVECONFLICT>
</IMPORTPARAMS>

```

**Hinweis:** Wenn Sie einen Objekttyp wiederverwenden oder ersetzen, überschreibt die Auflösung für diesen Objekttyp die Auflösung für alle Objekttypen. Im vorangehenden Beispiel werden Quelldefinitionen und Mappings ersetzt und die übrigen Objekte wiederverwendet. Verwenden Sie den Objekttyp "Alle", um alle Objekte wiederzuverwenden oder zu ersetzen. Weitere Informationen zu Objekttypen finden Sie unter ["Objektimport-Steuerdatei-Parameter" auf Seite 1554](#).

## Ersetzen ungültiger Mappings

Sie können ungültige Mappings sowie die zugehörigen untergeordneten Objekte ersetzen, die von einer Abfrage zurückgegeben wurden. Sie möchten beispielsweise Objekte ersetzen, die von der Abfrage QUERY\_PARENT\_RENAME zurückgegeben wurden.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```

<?xml version="1.0" encoding="UTF-16LE"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">

<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES"

CHECKIN_COMMENTS="PMREP_IMPORT_QUERY_PARENT_REPLACE_CHILD_REUSE"
APPLY_LABEL_NAME="LABEL_QUERY_PARENT_RENAME_CHILD_REUSE">
  <FOLDERMAP SOURCEFOLDERNAME="PMREP_CHECKED_OUT" SOURCEPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="PMREP_CHECKED_OUT" TARGETREPOSITORYNAME="REPO_EX_1"/>
  <RESOLVECONFLICT>

  <!--replace the objects returned by the query QUERY_PARENT_RENAME -->
  <QUERYOBJECT QUERYNAME="QUERY_PARENT_RENAME" RESOLUTION="REPLACE"/>
</RESOLVECONFLICT>
</IMPORTPARAMS>

```

## Umbenennen von Objekten

Sie können bestimmte Objekte umbenennen, wenn bei Objekten Konflikte auftreten. Sie möchten beispielsweise die Objekte ADDRESS, ADDRESS1, R\_LKP, MAP\_MLET, R\_S3, WF\_RS1 umbenennen. Der Repository Service hängt eine Zahl an den Objektnamen an.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```

<?xml version="1.0" encoding="UTF-16LE"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">

<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES"
CHECKIN_COMMENTS="PMREP_IMPORT_SPECIFICOBJECT_RENAME"
APPLY_LABEL_NAME="LABEL_IMPORT_SPECIFIC_OBJECT_RENAME">
  <FOLDERMAP SOURCEFOLDERNAME="SRC_FOLDER1" SOURCEPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="TGT_FOLDER1" TARGETREPOSITORYNAME="REPO_EX_1"/>

  <RESOLVECONFLICT>

  <!-- rename the objects ADDRESS, ADDRESS1, R_LKP, MAP_MLET, R_S3, WF_RS1 -->

  <SPECIFICOBJECT NAME="ADDRESS" DBDNAME="sol805" OBJECTTYPENAME="Source Definition"
FOLDERNAME="PMREP_CHECKED_OUT" REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
  <SPECIFICOBJECT NAME="ADDRESS1" OBJECTTYPENAME="Target Definition"

```

```

FOLDERNAME="PMREP_CHECKED_OUT" REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
<SPECIFICOBJECT NAME="R_LKP" OBJECTTYPE="Lookup_Procedure"
FOLDERNAME="PMREP_CHECKED_OUT" REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
<SPECIFICOBJECT NAME="MAP_MLET" OBJECTTYPE="Mapping" FOLDERNAME="PMREP_CHECKED_OUT"
REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
<SPECIFICOBJECT NAME="R_S3" OBJECTTYPE="Session" FOLDERNAME="PMREP_CHECKED_OUT"
REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
<SPECIFICOBJECT NAME="WF_RS1" OBJECTTYPE="Workflow" FOLDERNAME="PMREP_CHECKED_OUT"
REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
</RESOLVECONFLICT></IMPORTPARAMS>

```

## Kopieren von SAP-Mappings und SAP-Programminformationen

Sie können SAP-Programminformationen beim Importieren von SAP-Mappings kopieren. Sie möchten beispielsweise SAP-Mappings importieren und die Programminformationen kopieren, die dem in den Ordner TGT\_F1 zu importierenden Objekt zugeordnet sind.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```

<?xml version="1.0" encoding="UTF-16LE"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">

<!-- enter YES as the value for the COPY_SAP_PROGRAM attribute to copy SAP mappings and
SAP program information -->

<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="Version2 of objects"
APPLY_LABEL_NAME="LABEL71_REPLACE_FOLDER" COPY_SAP_PROGRAM="YES">
  <FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCE_REPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="TGT_F1" TARGET_REPOSITORYNAME="REPO_EX_1"/>
</IMPORTPARAMS>

```

## Anwenden von Standard-Verbindungsattributen

Sie können ein standardmäßiges Verbindungsattribut auf eine Sitzung anwenden, wenn im Target-Repository keine Verbindung existiert. Im Target-Repository REPO\_EX\_1 existiert beispielsweise keine Verbindung.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```

<?xml version="1.0" encoding="UTF-16LE"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">

<!-- enter YES as the value of the APPLY_DEFAULT_CONNECTION element to apply a default
connection attribute -->
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="NO" APPLY_DEFAULT_CONNECTION="YES">
  <FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCE_REPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="TGT_F1" TARGET_REPOSITORYNAME="REPO_EX_1"/>
<RESOLVECONFLICT>
<SPECIFICOBJECT NAME="R_S3" OBJECTTYPE="Session" FOLDERNAME="PMREP_CHECKED_OUT"
REPOSITORYNAME="REPO_EX_1" RESOLUTION="REPLACE"/>
<RESOLVECONFLICT>
</IMPORTPARAMS>

```

## Auflösen von Objektkonflikten

Sie können Objektkonflikte für beschriftete Objekte im Target-Repository auflösen. Sie verfügen beispielsweise über Mappings, Mapplets, Quellen und Targets mit der Beschriftung LBL\_MPNG\_MPLTS\_SRCS\_TGTS. Sie möchten diese Objekte ersetzen, mit der Beschriftung REPLACE\_LBL\_MPNG\_MPLTS\_SRCS\_TGTS versehen und alle Transformationen wiederverwenden.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```

<?xml version="1.0" encoding="UTF-16LE"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">

```

```

<IMPORTPARAMS CHECKIN AFTER IMPORT="YES" CHECKIN COMMENTS="PMREP_IMPORT_LABEL_REPLACE"
APPLY_LABEL_NAME="REPLACE_LBL_MPNG_MPLTS_SRCS_TGTS" >
<FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCE_REPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="TGT_F1" TARGET_REPOSITORYNAME="REPO_EX_1"/>

<!-- use the RESOLVECONFLICT element in conjunction with the RESOLUTION attribute of the
OBJECTTYPE element to resolve conflicts when you import objects -->
<RESOLVECONFLICT>
<LABELOBJECT LABELNAME="LBL_MPNG_MPLTS_SRCS_TGTS" RESOLUTION="REPLACE"/>
<TYPEOBJECT OBJECTTYPE="Lookup Procedure" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPE="Stored Procedure" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPE="Expression" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPE="Filter" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPE="Aggregator" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPE="Rank" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPE="Normalizer" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPE="Router" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPE="Sequence" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPE="Sorter" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPE="update strategy" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPE="Custom Transformation" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPE="Transaction control" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPE="External Procedure" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPE="Joiner" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPE="SessionConfig" RESOLUTION="REUSE"/>
</RESOLVECONFLICT>

</IMPORTPARAMS>

```

## Verwenden der Bereitstellungssteuerdatei

Eine Bereitstellungssteuerdatei ist eine XML-Datei, die Sie mit den *pmrep*-Befehlen "DeployFolder" und "DeployDeploymentGroup" verwenden, um einen Ordner oder eine Bereitstellungsgruppe bereitzustellen. Sie können eine Bereitstellungssteuerdatei manuell erstellen, um Parameter für die Bereitstellung anzugeben. Sie können sie aber auch mit dem Kopierassistenten erstellen.

Wenn Sie die Bereitstellungssteuerdatei manuell erstellen, muss sie der *depcntl.dtd*-Datei entsprechen, die mit dem PowerCenter Client installiert wird. Sie nehmen den Speicherort der *depcntl.dtd*-Datei in der Bereitstellungssteuerdatei auf.

Sie können in der Bereitstellungssteuerdatei einen Bereitstellungs-Timeout angeben. Der Bereitstellungs-Timeout ist der Zeitraum, den *pmrep* wartet, um Objektsperren im Target-Repository abzurufen. Standardmäßig wartet *pmrep* unbegrenzt, bis Sperren abgerufen werden oder Sie brechen die Bereitstellung ab. Wenn Sie eine Bereitstellung abbrechen möchten, während *pmrep* auf das Abrufen von Sperren wartet, drücken Sie Strg+C.

**Hinweis:** Sie müssen die Bereitstellungssteuerdatei manuell erstellen, um einige Bereitstellungsparameter wie *DEPLOYTIMEOUT* zu verwenden.

Im Folgenden sehen Sie ein Beispiel für eine *depcntl.dtd*-Datei:

```

<!ELEMENT DEPLOYPARAMS (DEPLOYFOLDER?, DEPLOYGROUP?)>
<!-- ATTLIST DEPLOYPARAMS
      DEFAULTSERVERNAME      CDATA      #IMPLIED
      COPYPROGRAMINFO        (YES | NO) "YES"
      COPYMAPVARIABLES       (YES | NO) "NO"
      RETAINMAPVARIABLES     (YES | NO) "NO"
      COPYFLOWVARIABLES      (YES | NO) "NO"
      COPYFLOWSESSLOGS       (YES | NO) "NO"
      COPYDEPENDENCY         (YES | NO) "YES"
      LATESTVERSIONONLY      (YES | NO) "NO"
      CHECKIN_COMMENTS       CDATA      #IMPLIED
-->

```



```

        DEPLOYTIMEOUT          CDATA          "-1"
        RETAINGENERATEDVAL      (YES | NO) "YES"
        RETAINSERVERNETVALS     (YES | NO) "YES"
        COPYDEPLOYMENTGROUP     (YES | NO) "NO"
        OVERRIDESESERVER        (YES | NO) "NO">

<!--criteria specific to deploying folder-->
<!ELEMENT DEPLOYFOLDER (REPLACEFOLDER?, DEPLOYEDFOLDEROWNER?, OVERRIDEFOLDER*)>
<!ATTLIST DEPLOYFOLDER
        NEWFOLDERNAME          CDATA          #IMPLIED>

<!--folder to replace-->
<!ELEMENT REPLACEFOLDER EMPTY>
<!ATTLIST REPLACEFOLDER
        FOLDERNAME             CDATA          #REQUIRED
        RETAINMAPVARPERVALS     (YES | NO) "NO"
        RETAINWFLOWVARPERVALS  (YES | NO) "YES"
        RETAINWFLOWSESSLOGS    (YES | NO) "NO"
        MODIFIEDMANUALLY        (YES | NO) "NO"
        RETAINORIGFOLDEROWNER   (YES | NO) "NO">

<!--shared folder to override-->
<!ELEMENT OVERRIDEFOLDER EMPTY>
<!ATTLIST OVERRIDEFOLDER
        SOURCEFOLDERNAME       CDATA          #REQUIRED
        SOURCEFOLDERTYPE        (LOCAL | GLOBAL) "LOCAL"
        TARGETFOLDERNAME       CDATA          #REQUIRED
        TARGETFOLDERTYPE        (LOCAL | GLOBAL) "LOCAL"
        MODIFIEDMANUALLY        (YES | NO) "NO"

<!--criteria specific to deploy deployment group-->
<!ELEMENT DEPLOYGROUP (REPLACEDG?, TARGETDGOWNER?, OVERRIDEFOLDER*, APPLYLABEL?)>
<!ATTLIST DEPLOYGROUP
        CLEARSRCDEPLOYGROUP     (YES | NO) "NO">
        NEWDEPLOYGROUPNAME      CDATA          #IMPLIED

<!--labels used to apply on the src objects and deployed objects-->
<!ELEMENT APPLYLABEL EMPTY>
<!ATTLIST APPLYLABEL
        SOURCELABELNAME         CDATA          #IMPLIED
        SOURCEMOVELABEL         (YES | NO) "NO"
        TARGETLABELNAME         CDATA          #IMPLIED
        TARGETMOVELABEL         (YES | NO) "NO">

<!-- new owners of deployed folders -->
<!ELEMENT DEPLOYEDFOLDEROWNER EMPTY>
<!ATTLIST DEPLOYEDFOLDEROWNER
        USERNAME                CDATA          #IMPLIED
        SECURITYDOMAIN           CDATA          #IMPLIED
        GROUPNAME               CDATA          #IMPLIED>

<!-- to indicate that a deployment group should be replaced-->
<!ELEMENT REPLACEDG EMPTY>
<!ATTLIST REPLACEDG
        DGNAME                  CDATA          #REQUIRED
        SECURITYDOMAIN           CDATA          #IMPLIED

<!-- new owner of copied deployment group-->
<!ELEMENT TARGETDGOWNER EMPTY>
<!ATTLIST TARGETDGOWNER
        USERNAME                CDATA          #IMPLIED
        SECURITYDOMAIN           CDATA          #IMPLIED

```

## Bereitstellungs-Steuerdatei-Parameter

In der folgenden Tabelle finden Sie eine Auflistung mit *pmrep*-Bereitstellungs-Steuerdatei-Parametern:

Element	Attributname	Attributbeschreibung
DEPLOYPARAMS	DEFAULTSERVERNAME	Erforderlich, wenn Sie DeployFolder und DeployDeploymentGroup verwenden und OVERRIDESERVER auf „Ja“ setzen. Der Integrationsdienst ist im Ziel-Repository zur Ausführung bereitgestellter Arbeitsabläufe registriert. Pro Bereitstellung können Sie einen Integrationsdienst angeben.
-	COPYPROGRAMINFO	Optional. Kopiert das mit SAP installierte ABAP-Programm.
-	COPYMAPVARPERVALS	Optional. Kopiert persistente Werte der Zuordnungsvariable basierend auf den für RETAINMAPVARPERVALS festgelegten Werten. Wenn Sie COPYMAPVARPERVALS nicht festlegen oder den zugehörigen Wert auf „Nein“ setzen, werden die Werte für RETAINMAPVARPERVALS ignoriert. Weitere Informationen hierzu finden Sie unter <a href="#">„Beibehaltene Zuordnungsvariablen“ auf Seite 1570</a> .
-	RETAINMAPVARPERVALS	Optional. Behält persistente Werte der Zuordnungsvariable basierend auf den für COPYMAPVARPERVALS festgelegten Werten im Ziel bei. Wenn Sie COPYMAPVARPERVALS nicht festlegen oder den zugehörigen Wert auf „Nein“ setzen, werden die Werte für RETAINMAPVARPERVALS ignoriert. Weitere Informationen hierzu finden Sie unter <a href="#">„Beibehaltene Zuordnungsvariablen“ auf Seite 1570</a> .
-	COPYFLOWVARPERVALS	Optional. Kopiert persistente Werte für die Arbeitsablaufvariable.
-	COPYFLOWSESSLOGS	Optional. Kopiert Arbeitsablaufprotokolle.
-	COPYDEPENDENCY	Optional. Kopiert Abhängigkeitsinformationen für Objekte in Zuordnungen.
-	COPYDEPLOYMENTGROUP	Optional. Kopiert die Bereitstellungsgruppe zusammen mit den Objekten in der Bereitstellungsgruppe in das Ziel-Repository.
-	VALIDATETARGETREPOSITORY	Optional. Validiert Objekte im Ziel-Repository.
-	LATESTVERSIONONLY	Optional. Kopiert die neueste Version.

Element	Attributname	Attributbeschreibung
-	CHECKIN_COMMENTS	Optional. Überschreibt den Standardkommentar und fügt einen Kommentar im Ziel-Repository beim Kopieren oder Bereitstellen eines Objekts hinzu. Sie müssen LATESTVERSIONONLY auf TRUE festlegen, um dieses Attribut zu verwenden.
-	DEPLOYTIMEOUT	Optional. Zeitraum (in Sekunden), in dem <i>pmrep</i> versucht, Sperren für Objekte im Ziel-Repository abzurufen. Bei einem Wert von 0 schlägt der Kopiervorgang sofort fehl, wenn <i>pmrep</i> keine Sperre erhält. Der Wert -1 weist <i>pmrep</i> an, so lange zu warten, bis die Sperren übermittelt werden oder der Benutzer den Vorgang abbricht. Standardwert ist -1.
-	RETAINGENERATEDVAL	Optional. Speichert den aktuellen Wert für Sequenzgenerator- oder Normalisierungsumwandlungen.
-	RETAINSERVERNETVALS	Optional. Behält Werte, die sich auf das Netzwerk oder den Server beziehen, in Aufgaben bei.
	OVERRIDESEVER	<p>Optional. Verwenden Sie dieses Attribut gemeinsam mit DEFAULTSERVERNAME. Wenn Sie den Wert OVERRIDESEVER auf „Yes“ setzen, weist der Bereitstellungsvorgang den Namen des Integrationsdiensts zu, der vom Attribut DEFAULTSERVERNAME zum Ausführen der bereitgestellten Arbeitsabläufe angegeben wird. Wenn der Wert DEFAULTSERVERNAME nicht angegeben ist oder einen ungültigen Namen für den Integrationsdienst aufweist, wird den bereitgestellten Arbeitsabläufen während der Bereitstellung kein Integrationsdienst zugewiesen.</p> <p>Wenn Sie den Wert OVERRIDESEVER auf „No“ setzen, wird während der Bereitstellung geprüft, ob ein Integrationsdienst basierend auf dem Integrationsdienst in den Quell- und Ziel-Repositorys zu den Arbeitsabläufen zugewiesen werden kann. Wenn derselbe Integrationsdienstname in den Quell- und Ziel-Repositorys angezeigt wird, erfolgt die Zuweisung des Integrationsdienstnamens zu den bereitgestellten Arbeitsabläufen während der Bereitstellung. Andernfalls werden dem Integrationsdienst die bereitgestellten Arbeitsabläufe nicht zugewiesen.</p> <p>Standardwert ist „No“.</p>

Element	Attributname	Attributbeschreibung
DEPLOYFOLDER	NEWFOLDERNAME	Optional. Erstellt einen Ordner mit diesem Namen.
REPLACEFOLDER	FOLDERNAME	Erforderlich, wenn Sie DEPLOYFOLDER verwenden. Benennt den Ordner, nachdem dieser ersetzt wurde.
-	RETAINMAPVARPERVALS	Optional. Behält persistente Werte für die Zuordnungsvariable im Ziel bei.
-	RETAINWFLOWVARPERVALS	Optional. Behält persistente Werte für Arbeitsablaufvariablen bei.
-	RETAINWFLOWSESSLOGS	Optional. Behält Sitzungsprotokolle des Arbeitsablaufs im Ziel bei.
-	MODIFIEDMANUALLY	Optional. Vergleicht Ordner, wenn Objekte im Zielordner seit der letzten Bereitstellung erstellt oder geändert wurden.
-	RETAINORIGFOLDEROWNER	Optional. Behält den vorhandenen Ordneigentümer bei. <i>pmrep</i> ignoriert alle im DEPLOYEDFOLDEROWNER-Element bereitgestellten Informationen.
OVERRIDEFOLDER	SOURCEFOLDERNAME	<p>Erforderlich, wenn Sie DeployFolder und DeployDeploymentGroup verwenden.</p> <p>Bei der Bereitstellung eines Ordners wird der aktuelle Ordner angegeben, auf den die Shortcuts zeigen.</p> <p>Bei der Bereitstellung einer Bereitstellungsgruppe werden die folgenden Ordner angegeben:</p> <ul style="list-style-type: none"> <li>- Ein oder mehrere Ordner, auf den bzw. die die Shortcuts zeigen</li> <li>- Ein oder mehrere Ordner mit den Bereitstellungsgruppenobjekten</li> </ul>
-	SOURCEFOLDERTYPE	Optional. Bei der Bereitstellung eines Ordners wird der Ordner typ angegeben, auf den die Shortcuts zeigen. Verwenden Sie lokale oder globale Shortcuts.
-	TARGETFOLDERNAME	<p>Erforderlich. Bei der Bereitstellung eines Ordners wird der Ordner angegeben, auf den die Shortcuts zeigen.</p> <p>Bei der Bereitstellung einer Bereitstellungsgruppe werden die folgenden Ordner angegeben:</p> <ul style="list-style-type: none"> <li>- Ein oder mehrere Ordner, auf den bzw. die die Shortcuts zeigen</li> <li>- Ein oder mehrere Ordner mit den Bereitstellungsgruppenobjekten</li> </ul>

Element	Attributname	Attributbeschreibung
-	TARGETFOLDERTYPE	Optional. Bei der Bereitstellung eines Ordners wird der Ordnertyp angegeben, auf den die Shortcuts zeigen. Verwenden Sie lokale oder globale Shortcuts.
-	MODIFIEDMANUALLY	Optional. Vergleicht Ordner, wenn Objekte im Zielordner seit der letzten Bereitstellung erstellt oder geändert wurden. Verwenden Sie dieses Attribut nur mit dem DeployDeploymentGroup-Befehl.
DEPLOYGROUP	CLEARSRCDPLOYGROUP	Erforderlich, wenn Sie DeployDeploymentGroup verwenden. Entfernt nach der Bereitstellung Objekte aus der Quellgruppe.
-	NEWDEPLOYGROUPNAME	Optional. Erstellt eine Bereitstellungsgruppe mit diesem Namen. Wird bei Angabe von REPLACEDG ignoriert. Standardwert ist der Name der Quellbereitstellungsgruppe.
REPLACEDG	DGNAME	Optional. Name der zu ersetzenden Bereitstellungsgruppe.
-	RETAINORIGDGOWNER	Optional. Gibt an, ob der Eigentümer der Bereitstellungsgruppe, die im Ziel-Repository ersetzt wurde, beibehalten werden soll.
TARGETDGOWNER	USERNAME	Optional. Eigentümer der kopierten Bereitstellungsgruppe. Standardwert ist der Eigentümer der Quellbereitstellungsgruppe.
-	SECURITYDOMAIN	Optional. Sicherheitsdomäne der Zielbereitstellungsgruppe.
APPLYLABEL	SOURCELABELNAME	Erforderlich, wenn Sie DeployDeploymentGroup verwenden. Wendet eine Beschriftung auf alle Objekte in der Quellgruppe an.
-	SOURCEMOVELABEL	Optional. Verschiebt die Beschriftung aus einer anderen Version des Objekts in der Quellgruppe in die Bereitstellungsgruppenversion des Objekts. Wenn der Repository Agent feststellt, dass die Beschriftung auf eine andere Version desselben Objekts angewendet wird, können Sie die Beschriftung in die ausgewählte Version des Objekts verschieben.
-	TARGETLABELNAME	Optional. Wendet eine Beschriftung auf alle im Ziel-Repository bereitgestellten Objekte an.

Element	Attributname	Attributbeschreibung
-	TARGETMOVELABEL	Optional. Verschiebt die Beschriftung aus einer anderen Version des Objekts in der Zielgruppe in die Bereitstellungsgruppenversion des Objekts. Wenn der Repository Agent feststellt, dass die Beschriftung auf eine andere Version desselben Objekts angewendet wird, können Sie die Beschriftung in die aktuelle Version des Objekts verschieben.
DEPLOYEDFOLDEROWNER	USERNAME	Erforderlich, wenn Sie DeployFolder und DeployDeploymentGroup verwenden. Eigentümer des bereitgestellten Ordners oder der Bereitstellungsgruppe im Ziel-Repository.
-	SECURITYDOMAIN	Optional. Name der Sicherheitsdomäne, der der Eigentümer des bereitgestellten Ordners oder der Bereitstellungsgruppe angehört.
-	GROUPNAME	Optional. Gruppeneigentümer des bereitgestellten Ordners oder der Bereitstellungsgruppe im Ziel-Repository.

## Beibehaltene Zuordnungsvariablen

Beim Bereitstellen eines Ordners oder einer Gruppe können Sie die Werte der beibehaltenen Zuordnungsvariablen aus dem Quell- in das Ziel-Repository kopieren, die Werte aus dem Ziel-Repository beibehalten oder die Werte zurücksetzen.

In der folgenden Tabelle wird die Konfiguration von COPYMAPVARPERVALS und RETAINMAPVARPERVALS zum Kopieren, Beibehalten oder Zurücksetzen der Werte beibehaltener Zuordnungsvariablen beschrieben:

Bereitstellungsverhalten	Konfiguration
Setzen Sie die Werte der beibehaltenen Zuordnungsvariable im Ziel-Repository zurück.	Setzen Sie COPYMAPVARPERVALS auf „Nein“.
Kopiert die Werte der Zuordnungsvariable aus dem Quell- in das Ziel-Repository.	Legen Sie die folgenden Optionen für die Parameterdatei fest: <ul style="list-style-type: none"> <li>- Setzen Sie COPYMAPVARPERVALS auf „Ja“.</li> <li>- Setzen Sie RETAINMAPVARPERVALS auf „Nein“.</li> </ul>
Behält die vorhandenen Werte der beibehaltenen Zuordnungsvariable im Ziel-Repository bei.	Legen Sie die folgenden Optionen für die Parameterdatei fest: <ul style="list-style-type: none"> <li>- Setzen Sie COPYMAPVARPERVALS auf „Ja“.</li> <li>- Setzen Sie RETAINMAPVARPERVALS auf „Ja“.</li> </ul>

# Bereitstellungs-Steuerdatei – Beispiele

Die im Code der Bereitstellungs-Steuerdatei angegebenen Parameter bestimmen die Aktionen, die stattfinden, wenn Sie die Befehle DeployFolder oder DeployDeploymentGroup in *pmrep* ausführen. Die folgenden Beispiele behandeln Instanzen, in denen die Befehle DeployFolder und DeployDeploymentGroup mit einer Bereitstellungs-Steuerdatei verwendet werden.

## Bereitstellen der aktuellen Version eines Ordners

Sie können die aktuelle Version eines Ordners bereitstellen und alle Abhängigkeiten einschließen. Sie müssen beispielsweise die aktuellen Werte in einer Sequenzgenerator-Transformation beibehalten und die Shortcuts für den Ordner "sc\_folder" auf den Ordner "new\_sc\_folder" anpassen. Nach dem Kopieren des Ordners möchten Sie ihn in "new\_year" umbenennen.

Sie möchten unter Umständen eine Steuerdatei mit folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE DEPLOYPARAMS SYSTEM "depctl.dtd">
<DEPLOYPARAMS DEFAULTSERVERNAME="info7261"
  COPYPROGRAMINFO="NO"
  COPYWFLOWVARPERVALS="NO"
  COPYWFLOWSESSLOGS="NO"
  COPYDEPENDENCY="YES"
  LATESTVERSIONONLY="NO">

  <REPLACEFOLDER FOLDERNAME="NEW_YEAR"
    RETAINMAPVARPERVALS="YES"/>

  <OVERRIDEFOLDER SOURCEFOLDERNAME="SC_FOLDER"
    OVERRIDEFOLDERNAME="NEW_SC_FOLDER"/>

</DEPLOYPARAMS>
```

## Bereitstellen der aktuellen Version einer Bereitstellungsgruppe

Sie können die aktuelle Version einer Bereitstellungsgruppe bereitstellen und die Objekte in der Bereitstellungsgruppe mit einer Beschriftung versehen. Sie möchten beispielsweise die Beschriftung NEW\_SRC\_LABEL\_NAME auf alle Objekte in der Quellgruppe und die Beschriftung NEW\_TGT\_LABEL\_NAME auf alle Objekte in der Target-Gruppe anwenden. Sie möchten unter Umständen eine Steuerdatei mit folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>
<!DOCTYPE DEPLOYPARAMS SYSTEM "depctl.dtd">
<DEPLOYPARAMS DEFAULTSERVERNAME="dg_sunga2_51880"
  COPYPROGRAMINFO="YES"
  COPYMAPVARPERVALS="YES"
  COPYWFLOWVARPERVALS="YES"
  COPYWFLOWSESSLOGS="NO"
  COPYDEPENDENCY="YES"
  LATESTVERSIONONLY="YES"
  RETAINGENERATEDVAL="YES"
  RETAINSERVERNETVALS="YES">
  <DEPLOYGROUP CLEARSRCDEPLOYGROUP="NO">
    <OVERRIDEFOLDER SOURCEFOLDERNAME="SRC_FOLDER1"
      SOURCEFOLDERTYPE="LOCAL"
      TARGETFOLDERNAME="TGT_FOLDER1"
      TARGETFOLDERTYPE="LOCAL"/>
      <APPLYLABEL SOURCELABELNAME="NEW_SRC_LABEL_NAME"
        SOURCEMOVELABEL="YES"
        TARGETLABELNAME="NEW_TGT_LABEL_NAME"
        TARGETMOVELABEL="YES" />
    </DEPLOYGROUP>
  </DEPLOYPARAMS>
```

## Auflisten mehrerer Quell- und Target-Ordner

Verwenden Sie das Element `OVERRIDEFOLDER` in der Steuerdatei, um mehrere Quell- und Target-Ordner aufzulisten. Verwenden Sie die Attribute `SOURCEFOLDERNAME` und `TARGETFOLDERNAME`, um die folgenden Ordner in den Quell- und Target-Repositories anzugeben:

- Der oder die Ordner, auf den bzw. die die Shortcuts zeigen
- Der oder die Ordner, in dem bzw. denen die Bereitstellungsgruppenobjekte enthalten sind

Beim Ausführen des Befehls `pmrep DeployDeploymentGroup`, verwendet der Bereitstellungsvorgang den rechten Target-Ordner, nachdem die Objekte in der Bereitstellungsgruppe überprüft wurden.

Wenn eine Bereitstellungsgruppe beispielsweise Objekte in zwei Ordnern mit Shortcuts zu einem dritten Ordner enthält, können Sie eine Steuerdatei mit drei Vorkommen von `OVERRIDEFOLDER` erstellen. Die folgende Beispielsteuerdatei stellt eine Bereitstellungsgruppe bereit, die Objekte in den Ordnern `OBJECTFOLDER1` und `OBJECTFOLDER2` enthält, in denen Shortcuts enthalten sind, die auf den Ordner `SHAREDSHORTCUT` zeigen.

```
<!DOCTYPE DEPLOYPARAMS SYSTEM "depctl.dtd">
<DEPLOYPARAMS DEFAULTSERVERNAME="dg_sun_71099"
  COPYPROGRAMINFO="YES"
  COPYMAPVARPERVALS="YES"
  COPYWFLOWVARPERVALS="YES"
  COPYWFLOWSESSLOGS="NO"
  COPYDEPENDENCY="YES"
  LATESTVERSIONONLY="YES"
  RETAINGENERATEDVAL="YES"
  RETAINSERVERNETVALS="YES">
  <DEPLOYGROUP CLEARSRCDEPLOYGROUP="NO">
    <OVERRIDEFOLDER SOURCEFOLDERNAME="OBJECTFOLDER1"
      SOURCEFOLDERTYPE="LOCAL"
      TARGETFOLDERNAME="OBJECTFOLDER1"
      TARGETFOLDERTYPE="LOCAL"/>
    <OVERRIDEFOLDER SOURCEFOLDERNAME="OBJECTFOLDER2"
      SOURCEFOLDERTYPE="LOCAL"
      TARGETFOLDERNAME="OBJECTFOLDER2"
      TARGETFOLDERTYPE="LOCAL"/>
    <OVERRIDEFOLDER SOURCEFOLDERNAME="SHAREDSHORTCUTS"
      SOURCEFOLDERTYPE="GLOBAL"
      TARGETFOLDERNAME="SHAREDSHORTCUTS"
      TARGETFOLDERTYPE="GLOBAL"/>
  </DEPLOYGROUP>
</DEPLOYPARAMS>
```

## Tipps für die Arbeit mit pmrep-Dateien

Verwenden Sie die Option `-n`, wenn Sie die `pmrep`-Befehle `"Updatesrcprefix"` oder `"Updatetargprefix"` verwenden.

Wenn Sie die Option `-n` angeben, müssen Sie den Namen der Quell- oder Target-Instanz für die Option `-t` eingeben. Der Quell- oder Target-Instanzname muss mit dem in den Sitzungseigenschaften angezeigten Namen oder dem vom `Listtablesbyess`-Befehl ausgegebenen Namen übereinstimmen.

Geben Sie die Option `-n` an, um den `Listtablesbyess`-Befehl mit dem `Updatesrcprefix`- oder dem `Updatetargprefix`-Befehl in einem Shell-Skript zu verwenden, wenn Quell- und Target-Instanznamen nicht übereinstimmen. Geben Sie außerdem die Option `-n` zum Aktualisieren einer Quelle an, selbst wenn die Sitzung einen Shortcut zum Mapping verwendet.



Geben Sie beim Verwenden des *pmrep* ListObjects-Befehls ein Zeichen oder eine Zeichenfolge ein, das bzw. die in Repository-Objektnamen nicht als Spaltentrennzeichen, Satzendeckennzeichen oder Endeckennzeichen der Auflistung verwendet wird.

Wenn Sie Zeichen eingeben, um Datensätze und Spalten zu trennen und das Ende einer Auflistung zu kennzeichnen, verwenden Sie Zeichen, die nicht in Repository-Objektnamen enthalten sind. Dies hilft bei der Verwendung eines Shell-Skripts zum Parsen der Objektmetadaten.

Verwenden Sie in *pmrep* die Option -v, wenn Sie ein Repository wiederherstellen, das einen externen Verzeichnisdienst für die Benutzerverwaltung einsetzt.

Wenn Sie die Option -v mit Restore verwenden, können Sie die externe Verzeichnisdienstregistrierung für das Repository beibehalten. Wenn Sie diese Option nicht mit dem gültigen Administratorbenutzernamen und -passwort eingeben, wird standardmäßig der Repository-Authentifizierungsmodus für das wiederhergestellte Repository verwendet und die Zuordnungen zwischen Anmeldenamen und Benutzernamen gehen verloren.

# INDEX

## A

### Abfragen

Ausführen [1480](#)

### Abfrageparameter

query [293](#)

### Abfragestruktur

query [295](#)

abortAllJobs (infacmd ms) [970](#)

abortRun (infacmd mi) [864](#)

aborttask (pmcmd)

Beschreibung [1397](#)

abortWorkflow

infacmd wfs [1237](#)

AbortWorkflow (pmcmd)

Beschreibung [1399](#)

Abrufen aggregierter Clusterprotokolle

infacmd ms [975](#)

AddAlertUser (infacmd isp) [367](#)

AddConnectionPermissions (infacmd isp) [369](#)

addCustomLDAPType (infacmd isp)

Beschreibung [371](#)

AddDomainLink (infacmd isp) [374](#)

AddDomainNode (infacmd isp) [376](#)

AddGroupPrivilege (infacmd isp) [378](#), [396](#)

addLDAPConnectivity (infacmd isp)

Beschreibung [380](#)

AddLicense (infacmd isp) [383](#)

AddNamespace (infacmd isp) [385](#)

AddNodeResource (infacmd isp) [388](#)

AddParameterSetEntries (infacmd dis) [157](#)

AddRolePrivilege (infacmd isp) [390](#)

AddServiceLevel (infacmd isp) [392](#)

AddToDeploymentGroup (pmrep)

Beschreibung [1447](#)

AddUserPrivilege (infacmd isp) [394](#)

ADLS-Zertifikat

Aktualisieren [99](#)

### Alarme

Abonnieren für Benutzer [367](#)

Aufheben des Abonnements mit infacmd isp [687](#)

Auflisten von eingetragenen Benutzern mit infacmd isp [602](#)

Auflisten von SMTP-Einstellungen mit infacmd [666](#)

Konfigurieren von SMTP-Einstellungen mit infacmd isp [813](#)

### Analyst Service

Audit-Verlauf für Unternehmensglossar löschen [88](#)

### Analyst-Dienst

Aktualisieren von Business Glossary-Daten [87](#)

Aktualisieren von Eigenschaften für [74](#)

Audit-Tabellen für Ausnahmeverwaltungsaufgaben erstellen [68](#)

Audit-Tabellen für Ausnahmeverwaltungsaufgaben löschen [72](#)

Auflisten der Konfiguration [73](#)

Auflisten von Eigenschaften für [73](#)

Auflisten von Unternehmensglossaren [89](#)

Erstellen in einer Domäne [70](#)

Exportieren von Unternehmensglossaren [90](#)

### Analyst-Dienst (Fortsetzung)

Importieren von Unternehmensglossaren aus XLSX-Dateien [92](#)

### Analyst-Dienst-Prozess

Konfigurieren von Eigenschaften für [75](#)

### Anwendungen

Auflisten von Objekten für [193](#)

Wiederherstellen [233](#)

### Anwendungsarchiv-Dateien (iar)

Bereitstellen im Datenintegrationsdienst [181](#)

### Anwendungsdienste

Abrufen des Status [582](#)

Abrufen von Eigenschaften [577](#)

aktivieren [1220](#)

Aktivieren [555](#)

Deaktivieren [544](#)

Entfernen mit infacmd isp [719](#)

### Anwendungsdienstprozesse

Abrufen des Status [580](#)

### Anwendungsobjekt

Auflisten von Berechtigungen für Benutzer oder Gruppen [191](#)

Einrichten von Berechtigungen [237](#)

### application

Auflisten von Berechtigungen [197](#)

Auflisten von Eigenschaften für [195](#)

Einrichten von Berechtigungen [234](#)

### Application

Aktualisieren [261](#)

Anhalten [246](#)

Bereinigen des Ergebnissatz-Caches [221](#)

Entfernen aus dem Datenintegrationsdienst [259](#)

Konfigurieren von Eigenschaften für [263](#)

Starten [244](#)

Umbenennen [228](#)

### ApplyLabel (pmrep)

Beschreibung [1449](#)

### Arbeitsablauf

Einrichten von Berechtigungen [237](#)

### Arbeitsablaufdienst

Entfernen von Datenbanktabellen [1249](#)

### Arbeitsabläufe

Abrufen von Protokollereignissen [591](#)

Anhalten über Befehlszeile [1431](#)

Auflisten [1261](#)

Starten über Befehlszeile [1425](#)

Wiederherstellen mithilfe der pmcmd-Syntax [1416](#)

### Arbeitsablaufprozessdaten

Löschen aus der Datenbank [1263](#)

AssignDefaultOSProfile (infacmd isp) [398](#)

AssignedToLicense (infacmd isp) [400](#)

AssignGroupPermission (infacmd isp) [402](#)

AssignIntegrationService (pmrep)

Beschreibung [1451](#)

AssignSToMMService (infacmd isp) [404](#)

AssignLicense (infacmd isp) [406](#)

AssignPermission (pmrep)

Beschreibung [1452](#)

- AssignRoleToGroup (infacmd isp) [408](#)
- AssignRoletoUser (infacmd isp) [410](#)
- AssignRSToWSHubService (infacmd isp) [412](#)
- AssignUserPermission (infacmd isp) [414](#)
- Audit-Trail-Tabellen
  - Erstellen, Content-Managementdienst [132](#)
  - Löschen, Content-Managementdienst [137](#)
- Ausführen einer Zuordnung
  - mit einem Laufzeitparametersatz [991](#)
- Ausführungszusammenfassung
  - bereitgestellte mi-Spezifikation [875](#)
- autotune
  - Dienste [85](#)
  - Domäne [85](#)
  - Verbindungen [85](#)

## B

- BackUp (pmrep)
  - Beschreibung [1454](#)
- BackupApplication (infacmd dis) [159](#)
- BackupContents (infacmd mrs) [884](#)
- BackupDomain (infasetup)
  - Beschreibung [1329](#)
- Befehle
  - Eingeben von Optionen und Argumenten für [37](#)
- Befehlszeilendienstprogramme
  - Datei „domains.inf“ [34](#)
  - konfigurieren [33](#)
- Befehlszeilendienstprogramme (Metadata Manager-Dienstprogramme konfigurieren) [34](#)
- Befehlszeilendienstprogramme (PowerCenter-Dienstprogramme konfigurieren) [33](#)
- Befehlszeilenmodus für pmcmd
  - Verbinden [1392](#)
- Befehlszeilenprogramme
  - Syntax für [38](#)
  - Übersicht [36](#)
- Benutzer
  - Auflisten mit infacmd isp [610](#)
  - Auflisten von Berechtigungstypen für [617](#)
  - Auflisten von Gruppen für einen Benutzer [638](#)
  - Entfernen aus einer Gruppe mit infacmd isp [725](#)
  - Entfernen mit infacmd isp [723](#)
  - Erstellen in einer Domäne [533](#)
  - Exportieren [563](#)
  - Exportieren mit infacmd isp [560](#)
  - Hinzufügen zu Gruppen in einer Domäne [396](#)
  - Importieren mit infacmd isp [595](#), [600](#)
  - Migrieren mit infacmd [674](#)
- Benutzer und Gruppen
  - Entfernen von Berechtigungen [737](#)
- Benutzer und Gruppen in der Sicherheitsdomäne
  - Synchronisieren mit LDAP-Benutzern und -Gruppen [749](#)
- Benutzerberechtigungen
  - Auflisten für Domänenobjekte [668](#)
- Benutzerkonten
  - Aktivieren [558](#)
  - Bearbeiten von Eigenschaften [550](#)
  - Deaktivieren in einer Domäne [548](#)
- Berechnungsknoten
  - Auflisten von Attributen für [1114](#)
  - Einrichten von Attributen [1117](#)
- Berechtigungen
  - Auflisten für Dienste mit infacmd isp [662](#)
  - Auflisten für eine Gruppe mit infacmd isp [636](#)
  - Auflisten für eine Rolle mit infacmd isp [655](#)

- Berechtigungen (*Fortsetzung*)
  - Auflisten für einen Benutzer [670](#)
  - Entfernen [1518](#)
  - Entfernen aus Benutzer- oder Gruppenverbindungen mit infacmd isp [691](#)
  - Entfernen aus einer Gruppe mit infacmd isp [704](#)
  - Entfernen aus einer Rolle mit infacmd isp [717](#)
  - Entfernen von einem Benutzer mit infacmd isp [729](#)
  - Zuweisen mit pmrep [1452](#)
  - Zuweisen zu Gruppen in einer Domäne [378](#)
  - Zuweisen zu Rollen [390](#)
- Bereitgestellte Anwendungen
  - Auflisten [199](#)
  - Sichern [159](#)
- Bereitstellen
  - Patch [1235](#)
- Bereitstellen von Objekten
  - depctl.dtd [1564](#)
- BereitstellungsGruppeBereitstellen (pmrep)
  - Beschreibung [1477](#)
- Bereitstellungsgruppen
  - Auflisten mehrerer Ordner [1572](#)
- Bereitstellungssteuerdatei
  - Beschreibung [1564](#)
- Beschreibung [682](#)
- Beschriftungen
  - Erstellen mit pmrep [1466](#)
  - Löschen [1475](#)
- Betriebssystemprofil
  - Aktualisieren mit infacmd isp [799](#)
  - Auflisten mit infacmd isp [652](#)
  - Auflisten von Standardprofilen [624](#)
  - Entfernen mit infacmd isp [713](#)
  - Entfernen von Standardprofil von einem Benutzer oder einer Gruppe [751](#)
  - Zuweisen von Standardprofil zu einem Benutzer oder einer Gruppe [398](#)
- Betriebssystemprofile
  - Erstellen in einer Domäne [517](#)
- Binäre Protokolldateien
  - Umwandeln in Text, XML oder lesbaren Text [417](#)
- Blaze-Dienst
  - Stoppen [248](#)

## C

- Cache für virtuelle Tabellen
  - Aktualisieren [1185](#)
  - Bereinigen [1183](#)
- CancelDataObjectCacheRefresh (infacmd dis) [161](#)
- cancelProfileExecution (infacmd ps) [1006](#)
- cancelWorkflow
  - infacmd wfs [1241](#)
- ChangeOwner (pmrep)
  - Beschreibung [1455](#)
- CheckIn (pmrep)
  - Beschreibung [1455](#)
- CheckInObject (infacmd mrs) [886](#)
- CI/CD-Richtlinien
  - infacmd dis [289](#)
- CleanUp (pmrep)
  - Beschreibung [1456](#)
- clearConfigurationProperties (infacmd cluster) [109](#)
- ClearDeploymentGroup (pmrep)
  - Beschreibung [1456](#)
- CloseForceListener (infacmd pwx) [1037](#)
- CloseListener (infacmd pwx) [1040](#)

- Cluster
  - auflisten [97](#)
  - löschen [95](#)
- cluster configuration
  - creating [102](#), [105](#)
- cluster configurations
  - user permissions [122](#)
- Cluster-Konfiguration
  - aktualisieren [123](#)
  - Bearbeiten [125](#), [127](#)
  - Eigenschaften auflisten [118](#)
  - Eigenschaften verwalten [109](#), [129](#)
  - exportieren [111](#)
  - Gruppenberechtigungen [115](#)
  - Löschen [107](#)
- Cluster-Konfigurationen
  - auflisten [120](#)
  - Exportieren mit infacmd isp [560](#)
  - Importieren mit infacmd isp [595](#)
- compareMapping
  - infacmd dis [166](#)
- compareObject
  - infacmd dis [170](#)
- completeTask
  - infacmd wfs [1243](#)
- CondenseLogger (infacmd pwx) [1043](#)
- Confluent Kafka-Verbindung
  - mit infacmd erstellen [435](#)
- Connect (pmcmd)
  - Beschreibung [1401](#)
- Connect (pmrep)
  - Beschreibung [1457](#)
- connections
  - updating using infacmd isp [764](#)
- Content Management Service
  - Auflisten von Eigenschaften für [139](#)
  - Upgrade erfolgt [154](#)
- Content-Management-Dienst
  - Bereinigen verwaister Referenzdaten [143](#)
- Content-Managementdienst
  - Aktualisieren der Optionen für [149](#)
  - Auflisten der Optionen für [141](#)
  - Entfernen mithilfe von infacmd cms [145](#)
  - Erstellen in einer Domäne [134](#)
  - Synchronisieren von Daten mit Master-CMS-Rechner [147](#)
- Content-Managementdienst-Prozess
  - Konfigurieren von Optionen für [152](#)
- ConvertLogFile (infacmd isp) [417](#)
- CPU-Profil
  - Berechnen mit infacmd isp [735](#)
- Create (pmrep)
  - Beschreibung [1459](#)
- CreateAuditTables (infacmd cms) [132](#)
- createConfiguration (infacmd cluster) [102](#), [105](#)
- CreateConnection (infacmd isp) [418](#)
- CreateConnection (pmrep)
  - Beschreibung [1460](#)
- CreateContent (infacmd tdm) [1218](#)
- CreateContents (infacmd mrs) [888](#)
- createdatamaps (infacmd pwx) [1046](#)
- CreateDeploymentGroup (pmrep)
  - Beschreibung [1464](#)
- CreateExceptionAuditTables (infacmd as) [68](#)
- CreateFolder (infacmd isp) [496](#)
- CreateFolder (pmrep)
  - Beschreibung [1464](#)
- CreateGrid (infacmd isp) [498](#)
- CreateGroup (infacmd isp) [500](#)

- CreateGroup (pmrep)
  - Beschreibung [1466](#)
- CreateIntegrationService (infacmd isp) [502](#)
- CreateLabel (pmrep)
  - Beschreibung [1466](#)
- CreateListenerService (infacmd pwx) [1049](#)
- CreateLoggerService (infacmd pwx) [1051](#)
- CreateMMService (infacmd isp) [513](#)
- CreateOSProfile (infacmd isp) [517](#)
- CreateProject (infacmd mrs) [890](#), [892](#)
- CreateRepositoryService (infacmd isp) [522](#)
- CreateRole (infacmd isp) [527](#)
- CreateSAPBWService (infacmd isp) [529](#)
- CreateSchedule (infacmd sch) [1130](#)
- CreateService (infacmd as) [70](#)
- CreateService (infacmd cms) [134](#)
- CreateService (infacmd dis) [163](#)
- CreateService (infacmd edp) [315](#)
- CreateService (infacmd idp) [304](#)
- CreateService (infacmd mas) [849](#)
- CreateService (infacmd mi) [866](#)
- CreateService (infacmd mrs) [894](#)
- CreateService (infacmd search) [1157](#)
- CreateService (infacmd tdm) [1212](#)
- CreateUser (infacmd isp) [533](#)
- CreateWH (infacmd ps) [1008](#)
- CreateWSHubService (infacmd isp) [536](#)

## D

- Datenintegrationsdienst
  - auflisten [204](#)
  - Auflisten von Berechnungseigenschaften [200](#)
  - Erstellen [163](#)
  - Konfigurieren von Berechnungseigenschaften [264](#)
  - Konfigurieren von Eigenschaften für [271](#)
- Datenintegrationsdienst-Prozess
  - Auflisten von Eigenschaften für [214](#), [217](#)
  - Konfigurieren von Eigenschaften für [285](#)
- Datenobjekt-Cache
  - Aktualisieren [227](#)
- Datenobjekte
  - Auflisten von Eigenschaften für [202](#)
  - Konfigurieren von Eigenschaften für [266](#)
- Dauerhafte Mapping-Ausgaben
  - Löschen mit infacmd ms [972](#)
- DB2
  - infacmd-Verbindungsoptionen [456](#)
- DefineDomain (infasetup)
  - Beschreibung [1332](#)
- DefineGatewayNode (infasetup)
  - Beschreibung [1342](#)
- DefineWorkerNode (infasetup)
  - Beschreibung [1349](#)
- delegateTask
  - infacmd wfs [1247](#)
- Delete (pmrep)
  - Beschreibung [1472](#)
- DeleteauditHistory (infacmd bg) [88](#)
- DeleteAuditTables (infacmd cms) [137](#)
- deleteClusters (infacmd ccps) [95](#)
- deleteConfiguration (infacmd cluster) [107](#)
- DeleteConnection (pmrep)
  - Beschreibung [1473](#)
- DeleteContents (infacmd mrs) [899](#)
- DeleteDeploymentGroup (pmrep)
  - Beschreibung [1474](#)

- DeleteDomain (infasetup)
  - Beschreibung [1353](#)
- DeleteExceptionAuditTables (infacmd as) [72](#)
- DeleteFolder (infacmd mrs) [901](#)
- DeleteFolder (pmrep)
  - Beschreibung [1474](#)
- DeleteLabel (pmrep)
  - Beschreibung [1475](#)
- deleteMappignPersistedOutputs
  - infacmd ms [972](#)
- DeleteNamespace (infacmd isp) [540](#)
- DeleteObject (pmrep)
  - Beschreibung [1475](#)
- DeleteParameterSetEntries (infacmd dis) [174](#), [207](#)
- DeleteProject (infacmd mrs) [903](#)
- DeleteSchedule (infacmd sch) [1137](#)
- depctl.dtd
  - Auflisten [1564](#)
- DeployApplication (infacmd dis) [181](#)
- DeployFolder (pmrep)
  - Beschreibung [1478](#)
- DeployImport (infacmd rtm) [1122](#)
- deployObjects
  - infacmd tools [1224](#)
- deployObjectsToFile
  - infacmd dis [177](#)
- deploySpec (infacmd mi) [870](#)
- detectOrphanResults (infacmd ps) [1010](#)
- Dienste
  - Auflisten mit infacmd isp [664](#)
  - Pingen [679](#)
- Dienstebenen
  - Aktualisieren mit infacmd isp [809](#)
  - Auflisten mit infacmd isp [659](#)
  - Entfernen mit infacmd isp [721](#)
  - Hinzufügen [392](#)
- Dienstprozesse
  - Aktivieren auf Knoten [556](#)
  - Deaktivieren auf einem Knoten [546](#)
- DisableNodeResource (infacmd isp) [542](#)
- DisableService (infacmd isp) [544](#)
- DisableService (infacmd tdm) [1221](#)
- DisableServiceProcess (infacmd isp) [546](#)
- DisableUser (infacmd isp) [548](#)
- Disconnect (pmcmd)
  - Beschreibung [1402](#)
- DisplayAllLogger (infacmd pwx) [1056](#)
- DisplayCPULogger (infacmd pwx) [1059](#)
- DisplayEventsLogger (infacmd pwx) [1062](#)
- DisplayMemoryLogger (infacmd pwx) [1065](#)
- DisplayRecordsLogger (infacmd pwx) [1068](#)
- displayStatsListener (infacmd pwx) [1071](#)
- DisplayStatusLogger (infacmd pwx) [1074](#)
- Domäne für verschiedene Versionen
  - Ausführen von pmcmd [1392](#)
  - Ausführen von pmrep [1442](#)
- Domänen
  - Aktualisieren mit infasetup [1367](#)
  - Aktualisieren von Eigenschaften mit infacmd isp [771](#)
  - Auflisten verlinkter Domänen mit infacmd isp [628](#)
  - Auflisten von Eigenschaften mit infacmd isp [630](#)
  - Entfernen von Links mit infacmd isp [695](#)
  - Erstellen mit infasetup [1332](#)
  - Löschen mit infasetup [1353](#)
  - Pingen [679](#)
  - Sichern mit infasetup [1329](#)
  - Wiederherstellen mit infasetup [1359](#)

- Domänengateway-Hosts
  - Pingen [679](#)
- Domänenüberwachung
  - Aktualisierungsoptionen [788](#)
  - Auflisten von Optionen [644](#)
- Domänenüberwachungsoptionen aktualisieren (infacmd isp) [788](#)
- Domänenüberwachungsoptionen auflisten (infacmd isp) [644](#)
- dropTables (infacmd wfs) [1249](#)
- DropWH (infacmd ps) [1011](#)
- DTD-Datei
  - Plug-In-Vorlage [1516](#)

## E

- EditUser (infacmd isp) [550](#)
- EditUser (pmrep)
  - Beschreibung [1480](#)
- EnableNodeResource (infacmd isp) [553](#)
- EnableService (infacmd isp) [555](#)
- EnableService (infacmd tdm) [1220](#)
- EnableServiceProcess (infacmd isp) [556](#)
- EnableUser (infacmd isp) [558](#)
- Enterprise Data Preparation Service
  - creating [315](#)
  - purge audit events [320](#)
  - updating [322](#)
  - upgrading [326](#)
- Entsperren
  - Gesperrtes Objekt [952](#)
- Execute (infacmd ps) [1013](#)
- executeProfile (infacmd ps) [1015](#)
- ExecuteQuery (pmrep)
  - Beschreibung [1480](#)
- ExecuteSQL (infacmd sql) [1168](#)
- Exit (pmrep)
  - Beschreibung [1482](#)
- Export (infacmd rtm) [1124](#)
- Export-Steuerdateien
  - Beispiele für Domänenobjekte [1324](#)
  - Beispiele für Model Repository-Objekte [1325](#)
  - Parameter für Domänenobjekte [1311](#)
  - Regeln und Richtlinien [1323](#)
  - Schemadateien [1309](#)
- exportConfiguration (infacmd cluster) [111](#)
- exportControl.xsd
  - infacmd-Steuerdateien [1309](#)
- ExportDomainObjects (infacmd isp)
  - Beschreibung [560](#)
- exportGlossary (infacmd bg) [90](#)
- exportObjects
  - infacmd tools [1226](#)
- exportResources
  - infacmd tools [1228](#)
- exportSpec
  - infacmd mi [871](#)
- Exportsteuerdateien
  - Benennungskonventionen [1310](#)
  - infacmd [1309](#)
  - Parameter für Modellrepository-Objekte [1312](#)
- ExportToPC (infacmd ipc) [357](#)
- ExportUsersAndGroups (infacmd isp) [563](#)
- Externe Sicherheitsmodule
  - Aufheben der Registrierung [1525](#)
  - Registrieren [1516](#)

## F

FileSwitchLogger (infacmd pwx) [1077](#)  
FindCheckout (pmrep)  
  Beschreibung [1482](#)  
Funktionen  
  validieren [819](#)  
Für einen Datenintegrationsdienst bereitgestellte Mappings  
  Ausführen [991](#)

## G

gateway  
  Aktualisieren von Informationen mit infacmd isp [775](#)  
GenerateAbapProgramToFile (pmrep)  
  Beschreibung [1484](#)  
GenerateEncryptionKey (infasetup)  
  beschreibung [1356](#)  
generateReadableViewXML  
  infacmd xrf [1307](#)  
genreusereportfrompc (infacmd ipc) [363](#)  
Gespeicherte Prozeduren  
  Auflisten von Berechtigungen [1178](#)  
  Einrichten von Berechtigungen [1194](#)  
GetConnectionDetails (pmrep)  
  Beschreibung [1484](#)  
getDomainObjectPermissions (infacmd aud) [77](#)  
getExecutionStatus (infacmd ps) [1017](#)  
GetFolderInfo (infacmd isp) [566](#)  
GetLastError (infacmd isp) [567](#)  
GetLog (infacmd isp) [570](#)  
GetMappingStatus  
  infacmd ms [977](#)  
GetNodeName (infacmd isp) [573](#)  
GetPasswordComplexityConfig (infacmd) [574](#)  
getPrivilegeAssociation (infacmd aud) [78](#)  
getProfileExecutionStatus (infacmd ps) [1019](#)  
GetRequestLog  
  infacmd ms [979](#)  
getrunningsessionsdetails (pmcmd)  
  Beschreibung [1403](#)  
getSamlConfig (infacmd)  
  Beschreibung [575](#)  
GetServiceDetails (pmcmd)  
  Beschreibung [1404](#)  
GetServiceOption (infacmd isp) [577](#)  
GetServiceProcessOption (infacmd isp) [578](#)  
GetServiceProcessStatus (infacmd isp) [580](#)  
getserviceproperties (pmcmd)  
  Beschreibung [1406](#)  
GetServiceStatus (infacmd isp) [582](#)  
GetSessionLog (infacmd isp) [584](#)  
Getsessionstatistics (pmcmd)  
  Beschreibung [1407](#)  
getSpecRunStats  
  infacmd mi [874](#)  
GetSystemLogDirectory (infacmd isp) [587](#)  
gettaskdetails (pmcmd)  
  Beschreibung [1409](#)  
getUserGroupAssociation (infacmd aud) [80](#), [81](#)  
getUsersPersonalInfo (infacmd aud) [82](#)  
getworkflowdetails (pmcmd)  
  Beschreibung [1411](#)  
GetWorkflowLog (infacmd isp) [591](#)  
Gitter  
  Aktualisieren zugewiesener Knoten mit infacmd isp [776](#)  
  Auflisten von Knoten mit infacmd isp [633](#)

Gitter (*Fortsetzung*)

  Entfernen mit infacmd isp [699](#)  
  Erstellen [498](#)  
Gleichzeitige Arbeitsabläufe  
  Anhalten über Befehlszeile [1431](#)  
  Starten über Befehlszeile [1425](#)  
Gruppen  
  Auflisten für einen Benutzer [638](#)  
  Auflisten mit infacmd isp [605](#)  
  Entfernen mit infacmd isp [700](#)  
  Erstellen in Domänen [500](#)  
  Exportieren [563](#)  
  Exportieren mit infacmd isp [560](#)  
  Importieren mit infacmd isp [595](#), [600](#)  
Gruppenberechtigungen  
  Auflisten für Domänenobjekte [634](#)  
  Entfernen für Objekte [702](#)  
  Zuweisen zu Objekten [402](#)

## H

HBase connections for MapR-DB  
  infacmd properties [469](#)  
Help (infacmd) [595](#)  
help (pmcmd)  
  Beschreibung [1415](#)  
Hilfe (pmrep)  
  Beschreibung [1486](#)  
Human-Task-Instanzen [1243](#)

## I

IBM DB2  
  Verbindungsstring, Beispiel [1443](#)  
ICMD\_JAVA\_OPTS  
  Konfigurieren [45](#)  
Im Datenintegrationsdienst bereitgestellte Arbeitsabläufe  
  abbrechen [1237](#)  
  Starten [1273](#)  
  wiederherstellen [1265](#)  
  Wird abgebrochen [1241](#)  
impcntl.dtd  
  Beschreibung [1553](#)  
Import (infacmd rtm) [1127](#)  
Import-Steuerdateien  
  Beispiele für Domänenobjekte [1324](#)  
  Beispiele für Model Repository-Objekte [1325](#)  
  Parameter für Domänenobjekte [1316](#)  
  Regeln und Richtlinien [1323](#)  
  Schemadateien [1309](#)  
importControl.xsd  
  infacmd-Steuerdateien [1309](#)  
ImportDomainObjects (infacmd isp)  
  Beschreibung [595](#)  
importGlossary (infacmd bg) [92](#)  
Importieren aus PowerCenter  
  Optionen [361](#)  
Importieren von Objekten  
  impcntl.dtd [1553](#)  
  ObjectImport XML-Beispiel [1557](#)  
importObjects  
  infacmd tools [1230](#)  
Importsteuerdateien  
  Benennungskonventionen [1310](#)  
  infacmd [1309](#)  
  Parameter für Modellrepository-Objekte [1318](#)

- ImportUsersAndGroups (infacmd isp)
  - Beschreibung [600](#)
- INFA\_CLIENT\_RESILIENCE\_TIMEOUT
  - Konfigurieren [46](#)
- INFA\_CODEPAGE\_NAME
  - Konfigurieren [47](#)
- INFA\_DEFAULT\_DATABASE\_PASSWORD
  - Konfigurieren [47](#)
- INFA\_DEFAULT\_DB\_TRUSTSTORE\_PASSWORD
  - konfigurieren [49](#)
- INFA\_DEFAULT\_DOMAIN
  - Konfigurieren [50](#)
- INFA\_DEFAULT\_DOMAIN\_PASSWORD
  - Konfigurieren [50](#)
- INFA\_DEFAULT\_DOMAIN\_USER
  - Konfigurieren [51](#)
- INFA\_DEFAULT\_PWX\_OSEPASSWORD
  - Konfigurieren [52](#)
- INFA\_DEFAULT\_PWX\_OSPASSWORD
  - Konfigurieren [53](#)
- INFA\_JAVA\_CMD\_OPTS
  - Konfigurieren [55](#)
- INFA\_NODE\_KEYSTORE\_PASSWORD
  - konfigurieren [57](#)
- INFA\_NODE\_TRUSTSTORE\_PASSWORD
  - konfigurieren [58](#)
- INFA\_PASSWORD
  - Konfigurieren [55](#)
- INFA\_REPCNX\_INFO
  - Konfigurieren [58](#)
- INFA\_REPOSITORY\_PASSWORD
  - Konfigurieren [59](#)
- infacmd
  - Anzeigen der Hilfe für Befehle [595](#)
  - Auflisten von Plugin-IDs [65](#)
  - Dienstprozessoptionen [511](#)
  - Integrationsdienst-Optionen [506](#), [956](#)
  - Knoten, Wechseln von Arbeitsknoten zu Gateway-Knoten [745](#)
  - Listet die Benutzer auf, die ein schwaches Passwort verwenden. [672](#)
  - Lizenzen, Aufheben der Zuweisung [754](#)
  - Rückgabewerte [67](#)
  - running commands [65](#)
  - SAP BW Service-Optionen [532](#)
  - SAP BW Service-Prozessoptionen [532](#)
  - Sicherheitsdomänen, Auflisten [657](#)
  - Steuerdateien [1309](#)
  - Trennen des Metadata Manager-Diensts [752](#)
  - Überprüfen des Status der Passwortkomplexität [574](#)
  - Versionsinformationen, Anzeigen [820](#)
  - Web Services Hub-Dienstoptionen [538](#)
- infacmd advanced
  - Validieren von Funktionen [819](#)
- infacmd as
  - Aktualisieren von Eigenschaften für den Analyst-Dienst [74](#)
  - Audit-Tabellen für Ausnahme erstellen [68](#)
  - Audit-Tabellen für Ausnahmen löschen [72](#)
  - Auflisten der Konfiguration für den Analyst-Dienst [73](#)
  - Auflisten von Eigenschaften für den Analyst-Dienst-Prozess [73](#)
  - Erstellen eines Analyst-Dienst in einer Domäne [70](#)
  - Konfigurieren von Eigenschaften für Analyst-Dienst-Prozess [75](#)
- infacmd autotune
  - Autotune [85](#)
- infacmd bg
  - Aktualisieren von Business Glossary-Daten im Modellrepository [87](#)
  - Auflisten von Unternehmensglossaren in Analyst [89](#)
  - Exportieren von Unternehmensglossaren aus dem Analyst Tool [90](#)

- infacmd bg (Fortsetzung)
  - Importieren von Unternehmensglossaren aus XLSX- oder ZIP-Dateien in das Analyst Tool [92](#)
  - Löschen des Audit-Verlaufs eines Glossars aus dem Analyst Tool [88](#)
- infacmd ccps
  - ADLS-Dienstprinzipalzertifikat [99](#)
  - Auflisten von Clustern [97](#)
  - Cluster löschen [95](#)
- infacmd cluster
  - Aktualisieren der Konfigurationseigenschaften [129](#)
  - Auflisten der Konfigurationsdateien für die Hadoop-Verteilung [113](#), [117](#)
  - Bearbeiten von Cluster-Konfigurationseigenschaften [127](#)
  - Cluster-Konfiguration exportieren [111](#)
  - Cluster-Konfigurationen auflisten [120](#)
  - Cluster-Konfigurationsberechtigungen bearbeiten [125](#)
  - Cluster-Konfigurationseigenschaften auflisten [118](#)
  - Cluster-Konfigurationsinformationen aktualisieren [123](#)
  - creating a cluster configuration [102](#), [105](#)
  - Gruppenberechtigungen für eine Cluster-Konfiguration [115](#)
  - Konfigurationseigenschaften löschen [109](#)
  - Löschen von Konfigurationsobjekten [107](#)
  - user permissions for a cluster configuration [122](#)
- infacmd cms
  - Aktualisieren der Optionen für Content-Managementdienst [149](#)
  - Auflisten der Optionen für den Content-Managementdienst-Prozess [141](#)
  - Auflisten von Optionen für Content Management Service [139](#)
  - Bereinigen verwaister Referenzdaten [143](#)
  - Entfernen des Content-Managementdienst aus einer Domäne [145](#)
  - Erstellen von Audit-Trail-Tabellen [132](#)
  - Erstellen von Content-Managementdienst in einer Domäne [134](#)
  - Konfigurieren von Optionen für den Content-Managementdienst-Prozess [152](#)
  - Löschen von Audit-Trail-Tabellen [137](#)
  - Synchronisieren von Daten [147](#)
  - Upgrade des Dienstes [154](#)
- infacmd dis
  - Aktualisieren der Parametersatzeinträge [269](#)
  - Aktualisieren des aktuellen Werts für das Sequenzdatenobjekt [241](#)
  - Aktualisieren des Datenobjekt-Caches [227](#)
  - Aktualisieren von Anwendungen [261](#)
  - Aktualisierung des logischen Datenobjekt-Cache stoppen [161](#)
  - Anhalten von Anwendungen [246](#)
  - Auflisten bereitgestellter Anwendungen [199](#)
  - Auflisten der Objekte in einem Parametersatz [209](#)
  - Auflisten von Anwendungsberechtigungen [197](#)
  - Auflisten von Berechnungseigenschaften [200](#)
  - Auflisten von Berechtigungen für Anwendungsobjekte für Benutzer oder Gruppen [191](#)
  - Auflisten von Eigenschaften der Datenobjekte [202](#)
  - Auflisten von Eigenschaften des Datenintegrationsdienst-Prozesses [217](#)
  - Auflisten von Eigenschaften für Anwendungen [195](#)
  - Auflisten von Eigenschaften für Sequenzobjekte [214](#)
  - Auflisten von Objekten für Anwendungen [193](#)
  - Auflisten von Parametersätzen in einer Anwendung [211](#)
  - Bereinigen des Caches für logische Datenobjekte [219](#)
  - Bereinigen des Ergebnissatz-Caches [221](#)
  - Bereitstellen von Anwendungsarchiv-Dateien (iar) [181](#)
  - CI/CD-Richtlinien [289](#)
  - compareMapping [166](#)
  - compareObject [170](#)
  - Datenobjektoptionen [268](#)
  - deployObjectsToFile [177](#)
  - Einrichten von Anwendungsberechtigungen [234](#)
  - Einrichten von Arbeitsablaufberechtigungen [237](#)
  - Einrichten von Berechtigungen für Anwendungsobjekte [237](#)



#### infacmd dis (Fortsetzung)

- Einrichten von Mapping-Berechtigungen [237](#)
- Entfernen von Anwendungen [259](#)
- Erstellen eines Datenintegrationsdiensts [163](#)
- Hinzufügen von Parametersatzeinträgen [157](#)
- Konfigurieren von Anwendungseigenschaften [263](#)
- Konfigurieren von Berechnungseigenschaften [264](#)
- Konfigurieren von Datenobjekteigenschaften [266](#)
- Konfigurieren von Eigenschaften für den Datenintegrationsdienst [271](#)
- Konfigurieren von Eigenschaften für den Datenintegrationsdienst-Prozess. [285](#)
- Listet Sequenzobjekte auf. [216](#)
- listPatchNames [212](#)
- Löschen von Parametersatzeinträgen [174](#), [207](#)
- query [290](#)
- queryDesignTimeObjects [223](#)
- queryRunTimeObjects [225](#)
- replaceAllTag [256](#)
- Sichern einer bereitgestellten Anwendung [159](#)
- Starten von Anwendungen [244](#)
- Stoppen des Blaze-Diensts [248](#)
- Tag [251](#)
- Umbenennen bereitgestellter Anwendungen [228](#)
- untag [254](#)
- Wiederherstellen von Anwendungen aus Backup-Dateien [233](#)
  - Zuordnungen auflisten
    - im Datenintegrationsdienst [204](#)
    - im DIS [204](#)

#### infacmd edp

- creating Enterprise Data Preparation Service [315](#)
- purging Enterprise Data Preparation audit events [320](#)
- updating Enterprise Data Preparation Service [322](#)
- upgrading Enterprise Data Preparation Service [326](#)

#### infacmd idp

- creating Interactive Data Preparation Service [304](#)
- updating Interactive Data Preparation Service [309](#)

#### infacmd ipc

- Exportieren von Objekten aus dem Modellrepository [357](#)
- Wiederverwendung eines Berichtsbereichs [363](#)

#### infacmd isp

- Abonnieren von Benachrichtigungen für Benutzer [367](#)
- Abrufen angegebener Protokollereignisse [570](#)
- Abrufen der neuesten Fehlermeldungen [567](#)
- Abrufen des Status eines Anwendungsdienstprozesses auf einem Knoten [580](#)
- Abrufen des Status eines Anwendungsdiensts [582](#)
- Abrufen des Verzeichnispfads des Systemprotokolls [587](#)
- Abrufen von Diensteseigenschaften [577](#)
- Abrufen von Integrationsdienst-Prozesseigenschaften [578](#)
- Abrufen von Knotennamen [573](#)
- Abrufen von Protokollereignissen für Arbeitsabläufe [591](#)
- Abrufen von Protokollereignissen für Sitzungen [584](#)
- Aktivieren von Anwendungsdiensten [555](#)
- Aktivieren von Benutzerkonten [558](#)
- Aktivieren von Dienstprozessen auf einem Knoten [556](#)
- Aktivieren von Ressourcen [553](#)
- Aktualisieren der Knotenrolle [796](#)
- Alarmer, Aufheben des Abonnements [687](#)
- Alarmer, Auflisten von eingetragenen Benutzern [602](#)
- Alarmer, Konfigurieren von SMTP-Einstellungen [813](#)
- Auflisten der Benutzer mit Verbindungsberechtigungen [617](#)
- Auflisten von Berechtigungen für Benutzer oder Gruppen für eine Verbindung [613](#)
- Auflisten von Diensten, die einer Lizenz zugewiesen sind [400](#)
- Auflisten von Domänenobjekten für Benutzer [668](#)
- Auflisten von Domänenobjekten für Gruppen [634](#)
- Auflisten von Gruppen für einen Benutzer [638](#)

#### infacmd isp (Fortsetzung)

- Auflisten von Knotenrollen [648](#)
- Auflisten von Ordneigenschaften [566](#)
- Auflisten von SMTP-Einstellungen für den ausgehenden Mailserver [666](#)
- Auflisten von Standardbetriebssystemprofilen [624](#)
- Bearbeiten von Benutzerkontoeigenschaften [550](#)
- Benutzer und Gruppen, Exportieren [560](#)
- Benutzer und Gruppen, Importieren [595](#), [600](#)
- Benutzer, Auflisten [610](#)
- Benutzer, Auflisten von Berechtigungen für [670](#)
- Benutzer, Entfernen [723](#)
- Benutzer, Entfernen aus einer Gruppe [725](#)
- Benutzer, Entfernen von Berechtigungen [729](#)
- Berechtigungen, Entfernen aus Benutzer- oder Gruppenverbindungen [691](#)
- Betriebssystemprofil, Aktualisieren [799](#)
- Betriebssystemprofil, Auflisten [652](#)
- Betriebssystemprofil, Entfernen [713](#)
- Cluster-Konfigurationen, exportieren [560](#)
- Cluster-Konfigurationen, Importieren [595](#)
- connections, updating properties [764](#)
- CPU-Profil, Berechnen [735](#)
- Deaktivieren von Anwendungsdiensten [544](#)
- Deaktivieren von Benutzerkonten [548](#)
- Deaktivieren von Dienstprozessen auf einem Knoten [546](#)
- Deaktivieren von PowerCenter-Ressourcen [542](#)
- Dienste, Auflisten [664](#)
- Dienste, Berechtigungen auflisten [662](#)
- Dienste, Entfernen [719](#)
- Dienstebene, Aktualisieren [809](#)
- Dienstebenen, Auflisten [659](#)
- Dienstebenen, Entfernen [721](#)
- Dienstprozesse, Aktualisieren [810](#)
- Domänen, Aktualisieren von Eigenschaften [771](#)
- Domänen, Auflisten verlinkter Domänen [628](#)
- Domänen, Auflisten von Eigenschaften [630](#)
- Domänen, Entfernen von Links [695](#)
- Entfernen von Benutzerberechtigungen für Objekte [726](#)
- Entfernen von Berechtigungen für Benutzer und Gruppen [737](#)
- Entfernen von Gruppenberechtigungen für Objekte [702](#)
- Entfernen von Standardbetriebssystemprofil [751](#)
- Erstellen des Integrationsdiensts in einer Domäne [502](#)
- Erstellen des Repository-Diensts in einer Domäne [522](#)
- Erstellen des SAP BW-Dienst in einer Domäne [529](#)
- Erstellen einer Verbindung [418](#)
- Erstellen eines Metadata Manager-Diensts in einer Domäne [513](#)
- Erstellen eines Webdienst-Hub in einer Domäne [536](#)
- Erstellen von Benutzern in einer Domäne [533](#)
- Erstellen von Betriebssystemprofilen in einer Domäne [517](#)
- Erstellen von Gittern [498](#)
- Erstellen von Gruppen in Domänen [500](#)
- Erstellen von Ordnern [496](#)
- Erstellen von Rollen in einer Domäne [527](#)
- Exportieren von Benutzern und Gruppen in eine Datei [563](#)
- Exportsteuerdateien [1310](#)
- Gateway-Informationen, Aktualisieren [775](#)
- Gitter, Aktualisieren zugewiesener Knoten [776](#)
- Gitter, Auflisten von Knoten [633](#)
- Gitter, Entfernen [699](#)
- Gruppen, Auflisten [605](#)
- Gruppen, Auflisten von Berechtigungen für [636](#)
- Gruppen, Entfernen [700](#)
- Gruppen, Entfernen von Berechtigungen [704](#)
- Hinzufügen eines Domänenlinks [374](#)
- Hinzufügen von Benutzern zu Gruppen in einer Domäne [396](#)
- Hinzufügen von Dienstebenen [392](#)
- Hinzufügen von Knoten zu einer Domäne [376](#)



#### infacmd isp (Fortsetzung)

- Hinzufügen von Lizenzen zu Domänen [383](#)
- Hinzufügen von Ressourcen zu Knoten [388](#)
- Importsteuerdateien [1315](#)
- Integrationsdienste, Aktualisieren [778](#)
- Knoten, Aktualisieren [794](#)
- Knoten, Auflisten [650](#), [660](#)
- Knoten, Auflisten von Optionen [645](#)
- Knoten, Entfernen [710](#)
- Knoten, Herunterfahren [744](#)
- Knoten, Trennen von Domänen [762](#)
- Knoten, Wechseln von Gateway-Knoten zu Arbeitsknoten [747](#)
- Konfigurationslisten mit Chiffre-Suites anzeigen [625](#)
- LDAP-Authentifizierung, Einrichten [371](#), [380](#), [768](#), [781](#)
- LDAP-Serverkonfiguration, Aktualisieren [739](#)
- LDAP-Serverkonfiguration, Auflisten [654](#)
- LDAP-Verbindung, Auflisten [604](#), [607](#), [622](#), [640](#), [693](#), [706](#)
- Lizenzen, Aktualisieren [784](#)
- Lizenzen, Anzeigen von Informationen [742](#)
- Lizenzen, Auflisten [642](#)
- Lizenzen, Entfernen [708](#)
- Metadata Manager-Dienst-Eigenschaften, Aktualisieren [786](#)
- Migrieren von Benutzern [674](#)
- Ordner, Aktualisieren der Beschreibung [773](#)
- Ordner, Auflisten [631](#)
- Ordner, Entfernen [697](#)
- Ordner, Verschieben [675](#)
- Ordner, Verschieben von Objekten zwischen [677](#)
- Passwörter, Zurücksetzen von Benutzerpasswörtern [733](#)
- Ping-Domäne [680](#)
- Pingen von Objekten [679](#)
- Protokollereignisse, Bereinigen [683](#)
- Repository-Dienste, Aktualisieren [802](#)
- Ressourcen, Auflisten für Knoten [647](#)
- Ressourcen, Entfernen aus Knoten [711](#)
- Rollen, Auflisten [608](#)
- Rollen, Auflisten von Berechtigungen für [655](#)
- Rollen, Entfernen [715](#)
- Rollen, Entfernen aus einer Gruppe [756](#)
- Rollen, Entfernen von Benutzern [758](#)
- Rollen, Entfernen von Berechtigungen [717](#)
- Rollen, Exportieren [560](#)
- Rollen, Importieren [595](#)
- SAP BW Services, Aktualisieren [807](#)
- Synchronisieren von Benutzern und Gruppen in der Sicherheitsdomäne mit LDAP-Benutzern und -Gruppen [749](#)
- Umbenennen von Verbindungen [731](#)
- Umwandeln von binären Protokolldateien [417](#)
- Verbinden eines Repository mit Webdienst-Hub [412](#)
- Verbindungen, Auflisten [619](#)
- Verbindungen, Auflisten von Optionen [611](#), [621](#)
- Verbindungen, Entfernen aus Domänen [689](#)
- Verbindungen, Exportieren [560](#)
- Verbindungen, Importieren [595](#)
- Verbindungsberechtigungen, Auflisten nach Gruppe [615](#)
- Web Services Hub, Aktualisieren [815](#)
- Web Services Hub, Trennen eines Repository [760](#)
- Zuordnen von Rollen zu Gruppen für Domänen oder Anwendungsdienste [408](#)
- Zuweisen des Integrationsdiensts [404](#)
- Zuweisen von Benutzerberechtigungen zu Objekten [414](#)
- Zuweisen von Berechtigungen zu Benutzern [394](#)
- Zuweisen von Berechtigungen zu Gruppen [378](#)
- Zuweisen von Gruppenberechtigungen zu Objekten [402](#)
- Zuweisen von Lizenzen zu Anwendungsdiensten [406](#)
- Zuweisen von Privilegien zu Rollen in Gruppen [390](#)
- Zuweisen von Rollen zu Benutzern [410](#)
- Zuweisen von Standardbetriebssystemprofil [398](#)

#### infacmd isp (Fortsetzung)

- Zuweisen von Verbindungsberechtigungen zu Benutzern oder Gruppen [369](#)

#### infacmd mas

- Auflisten der Eigenschaften des Metadaten-Zugriffsdienst-Prozesses [855](#)
- Auflisten der Eigenschaften des Metadaten-Zugriffsdiensts [853](#)
- Erstellen des Metadaten-Zugriffsdiensts [849](#)
- Konfigurieren der Eigenschaften des Metadaten-Zugriffsdienst-Prozesses [860](#)
- Konfigurieren der Eigenschaften für den Metadaten-Zugriffsdienst [857](#)

#### infacmd mi

- Abbrechen einer Massenerfassungsspezifikation [864](#)
- Abrufen der Spezifikationsstatistiken [874](#)
- Auflistung der mi-Spezifikationen [876](#)
- Bereitstellen der Massenerfassungsspezifikation [870](#)
- Erstellen eines Massenerfassungsdiensts [866](#)
- extendedRunStats [872](#)
- listSpecRuns [875](#)
- Neustarten von Aufträgen [877](#)
- running mi spec [879](#)
- Spezifikationen bereitstellen [871](#)

#### infacmd mrs

- Aktualisieren der Statistik des Modellrepository-Diensts [963](#)
- Aktualisieren von Dienstprozessoptionen für den Modellrepository-Dienst [961](#)
- Aktualisieren von Optionen für den Modellrepository-Dienst [954](#)
- Auflisten von ausgecheckten Objekten [915](#)
- Auflisten von Berechtigungen für verschiedene Projekte [923](#)
- Auflisten von Dateien im Backup-Ordner [913](#)
- Auflisten von Dienstprozess-Optionen für den Modellrepository-Dienst [929](#)
- Auflisten von gesperrten Objekten [919](#)
- Auflisten von Optionen für den Modellrepository-Dienst [927](#)
- Auflisten von Ordnern im Repository des Modellrepository-Diensts [917](#)
- Auflisten von Projekten im Repository des Modellrepository-Dienst [925](#)
- Einchecken von Objekten [886](#)
- Entsperren eines Objekts [952](#)
- Erstellen des Modellrepository-Dienst [894](#)
- Erstellen eines Projekts [890](#), [892](#)
- Erstellen von Repository-Inhalt für einen Modellrepository-Dienst [888](#)
- Erstellt die Objektabhängigkeitsgrafik neu. [938](#)
- Füllen des Versionsverwaltungssystems [935](#)
- Löschen des Inhalts des Modellrepository [899](#)
- Löschen eines Ordners [901](#)
- Löschen eines Projekts [903](#)
- managing group permissions on project [931](#)
- managing user permissions on project [933](#)
- Neuzuweisung eines ausgecheckten Objekts [936](#)
- Neuzuweisung eines gesperrten Objekts [936](#)
- Sichern des Inhalts des Modellrepository in einer Datei [884](#)
- Umbenennen eines Ordners [940](#)
- Upgraden von Inhalten des Modellrepository-Dienst [965](#)
- Wiederherstellen der Inhalte des Modellrepository [944](#)
- Wiederherstellen von ausgecheckten Objekten [946](#), [950](#)
- Zuordnungen für den Modellrepository-Dienst auflisten [921](#)

#### infacmd ms

- Abrufen aggregierter Clusterprotokolle [975](#)
- Abrufen des Mapping-Status [977](#)
- Aktualisieren der Zuordnungsparameterdatei [1002](#)
- Auflisten der Mappings in einer Anwendung [987](#)
- Ausführen eines für einen Datenintegrationsdienst bereitgestellten Mappings [991](#)
- Jobs des Datenintegrationsdiensts abbrechen [970](#)

#### infacmd ms (Fortsetzung)

- Listet Zuordnungsoptionen in einer Anwendung auf [981](#)
- Löschen dauerhafter Zuordnungsausgaben [972](#)
- Optimierungsebene in einer Anwendung oder Zuordnung aktualisieren [1000](#)
- Schreiben des Zuordnungsprotokolls [979](#)
- Standardmäßige Optimierungsebene in einer Anwendung oder Zuordnung aktualisieren [998](#)
- Zeilen aus der Jobtabelle der Datenbank löschen [989](#)
- Zuordnungsoptionen in einer Anwendung aktualisieren [996](#)

#### infacmd oie

- Exportsteuerdateien [1310](#)
- Importsteuerdateien [1315](#)

#### infacmd ps

- Abrufen des Profilaufgabenstatus [1017](#)
- Abrufen des Profilmodellstatus [1019](#)
- Auflisten von Profil- und Scorecard-Ergebnissen [1021](#)
- Ausführen eines Profilmodells [1015](#)
- Ausführen von Profil- und Scorecard-Ergebnissen [1013](#)
- Bereinigen von Profil- und Scorecard-Ergebnissen [1028](#)
- Entfernen von Profiling Warehouse-Inhalten [1011](#)
- Erstellen eines Data Profiling Warehouse [1008](#)
- gcanceling Profilmodell [1006](#)
- Migrieren von Profilergebnissen [1024](#)
- Migrieren von Schlüsseln [1034](#)
- Migrieren von Scorecard-Ergebnissen [1026](#)

#### infacmd pwx

- Aktualisieren von Listenerdienst-Eigenschaften [1092](#)
- Aktualisieren von Protokollierungsdienst-Eigenschaften [1096](#)
- Anhalten des Listenerdiensts [1040](#)
- Anhalten des Protokollierungsdiensts [1083](#)
- Anhalten von Listenerdienst-Aufgaben [1086](#)
- Anzeigen aller Protokollierungsdienst-Nachrichten [1056](#)
- Anzeigen der Anzahl der vom Protokollierungsdienst verarbeiteten Änderungsdatensätze [1068](#)
- Anzeigen der Speichernutzung für den Protokollierungsdienst [1065](#)
- Anzeigen des Status der Writer-Unteraufgabe für Protokollierungsdienst [1074](#)
- Anzeigen von CPU-Informationen für den Protokollierungsdienst. [1059](#)
- Anzeigen von Ereignissen für den Protokollierungsdienst [1062](#)
- Anzeigen von Informationen für aktive Listenerdienst-Aufgaben [1080](#)
- Anzeigen von Überwachungsstatistiken für den Listenerdienst und dessen Aufgaben [1071](#)
- Erstellen des Listenerdiensts [1049](#)
- Erstellen des Protokollierungsdiensts [1051](#)
- Erstellen von Datenzuordnungen [1046](#)
- Erzwingen des Abbruchs des Listenerdiensts [1037](#)
- Starten des Protokollierungszyklus für den Protokollierungsdienst [1043](#)
- Upgraden nichtrelationaler Datenobjekte [1089](#)
- Wechseln zum neuen Satz an Protokolldateien des Protokollierungsdiensts [1077](#)

#### infacmd rms

- Auflisten von Attributen des Berechnungsknotens [1114](#)
- Auflisten von Eigenschaften für den Ressourcenmanager-Dienst [1116](#)
- Einrichten von Attributen des Berechnungsknotens [1117](#)
- Konfigurieren von Eigenschaften für Ressourcenmanager-Dienst [1119](#)

#### infacmd roh

- listProcessProperties [1101](#)
- listServiceOptions [1106](#)
- listServiceProcessOptions [1104](#)

#### infacmd rtm

- Exportieren von Referenztabelle [1124](#)
- Importieren von Inhalt aus Anwendungsdateien [1122](#)

#### infacmd rtm (Fortsetzung)

- Importieren von Referenztabelle in Modellrepositorys [1127](#)

#### infacmd sch

- Aktualisieren eines Zeitplans [1146](#)
- Erstellen eines Zeitplans [1130](#)
- Löschen eines Zeitplans [1137](#)

#### infacmd search

- Auflisten von Eigenschaften für den Suchdienst [1160](#)
- Auflistung der Eigenschaften für den Suchdienstprozess [1162](#)
- Konfigurieren von Eigenschaften für den Suchdienstprozess [1166](#)
- Konfigurieren von Eigenschaften für den Suchdienst [1164](#)
- Suchdienst wird erstellt [1157](#)

#### infacmd sql

- Aktualisieren des Caches für virtuelle Tabellen [1185](#)
- Aktualisieren von SQL-Datendienst-Optionen [1206](#)
- Anhalten des SQL-Datendienstes [1201](#)
- Auflisten der SQL-Datendienste für einen Datenintegrationsdienst [1176](#)
- Auflisten von Berechtigungen für einen SQL-Datendienst [1175](#)
- Auflisten von Berechtigungen für gespeicherte Prozeduren [1178](#)
- Auflisten von Berechtigungen für virtuelle Spalten [1171](#)
- Auflisten von Berechtigungen für virtuelle Tabellen [1182](#)
- Auflisten von Eigenschaften für einen SQL-Datendienst [1173](#)
- Auflisten von Eigenschaften für Spalten in virtuellen Tabellen [1169](#)
- Auflisten von Eigenschaften für virtuelle Tabellen [1180](#)
- Bereinigen des Caches für virtuelle Tabellen [1183](#)
- Einrichten von Benutzer- und Gruppenberechtigungen für gespeicherte Prozeduren [1194](#)
- Einrichten von Berechtigungen für einen SQL-Datendienst [1191](#)
- Einrichten von Berechtigungen in Spalten für virtuelle Tabellen [1189](#)
- Einrichten von Gruppen- und Benutzerberechtigungen für virtuelle Tabellen [1197](#)
- Konfigurieren von Eigenschaften für virtuelle Tabellen [1209](#)
- Spaltenoptionen [1205](#)
- SQL-Datendienst-Optionen [1207](#)
- Starten des SQL-Datendienstes [1199](#)
- Umbenennen des SQL-Datendienstes [1187](#)
- Virtuelle Tabellenoptionen [1211](#)

#### infacmd sqlupdate, Optionen für virtuelle Spalten [1203](#)

#### infacmd tdm

- Aktivieren des Test Data Manager-Diensts [1220](#)
- Deaktivieren des Test Data Manager-Diensts [1221](#)
- Test Data Manager-Dienste in einer Domäne erstellen [1212](#)
- Test Data Manager-Dienstinhalte in einer Domäne erstellen [1218](#)

#### infacmd tools

- Exportieren von Objekten [1226](#)
- Exportieren von Ressourcen nach Metadata Manager [1228](#)
- Importieren von Objekten [1230](#)
- Objekte werden bereitgestellt [1224](#)
- patchApplication [1235](#)

#### infacmd wfs

- Aktualisieren dauerhafter Zuordnungsausgaben [1269](#)
- Auflisten aktiver Arbeitsablaufinstanzen [1251](#)
- Auflisten dauerhafter Zuordnungsausgaben [1253](#)
- Auflisten der Arbeitsabläufe in einer Anwendung [1261](#)
- Auflisten von Arbeitsablaufparametern [1258](#)
- Auflisten von Human-Task-Instanzen [1255](#)
- eine Arbeitsablaufinstanz abbrechen [1241](#)
- eine Arbeitsablaufinstanz stornieren [1237](#)
- eine Arbeitsablaufinstanz wiederherstellen [1265](#)
- Entfernen von Datenbanktabellen [1249](#)
- Human-Task in einem Arbeitsablauf starten [1272](#)
- Human-Task-Instanz abschließen [1243](#)
- Human-Task-Instanz delegieren [1247](#)
- Human-Task-Instanz freigeben [1267](#)
- Prozessdaten aus der Arbeitsablaufdatenbank löschen [1263](#)
- Starten einer Ablaufinstanz [1273](#)

## infacmd ws

- Aktualisieren von Eigenschaften für einen Webdienst [1303](#)
- Aktualisieren von Eigenschaften für einen Webdienstvorgang [1300](#)
- Auflisten der Berechtigungen für einen Webdienst [1285](#)
- Auflisten der Berechtigungen für einen Webdienstvorgang [1281](#)
- Auflisten von Eigenschaften für einen Webdienstvorgang. [1279](#)
- ListOperationOptions [1279](#)
- ListOperationPermissions [1281](#)
- ListWebServiceOptions [1283](#)
- ListWebServicePermissions [1285](#)
- ListWebServices [1287](#)
- RenameWebService [1289](#)
- SetOperationPermissions [1291](#)
- SetWebServicePermissions [1294](#)
- StartWebService [1297](#)
- StopWebService [1299](#)
- UpdateOperationOptions [1300](#)
- UpdateWebServiceOptions [1303](#)

## infacmd xrf

- Aktualisieren von Export-XML [1308](#)
- Generieren einer lesbaren XML-Datei [1307](#)

## Infacmd-Befehle

- Abrufen der Hilfe [595](#)

## infasetup

- Aktivieren oder Deaktivieren der Passwortkomplexität [1376](#)
- Arbeitsknoten, Aktualisieren [1379](#)
- Arbeitsknoten, Definieren [1349](#)
- ausführen [1328](#)
- Chiffre-Suites aktualisieren [1364](#)
- displaying the cipher suite lists [1357](#)
- Domäne, aktualisieren [1384](#)
- Domäne, Definieren [1332](#)
- Domäne, Löschen [1353](#)
- Domäne, Sichern [1329](#)
- Domäne, Wiederherstellen [1359](#)
- Domänen, aktualisieren [1367](#)
- Gateway-Knoten, Aktualisieren [817](#), [1367](#), [1386](#)
- Gateway-Knoten, Definieren [1342](#)
- Rückgabewerte [1328](#)

## INFATool\_DATEFORMAT

- Konfigurieren [60](#)

## Informatica-Dienstprogramme (Installieren [32](#))

## Informatica-Dienstprogramme (Sicherheitskonfiguration [35](#))

## Inhalt

- Importieren aus Anwendungsdateien [1122](#)

## InstallAbapProgram (pmrep)

- Beschreibung [1486](#)

## Integrationsdienst

- Aktualisieren mit infacmd isp [778](#)
- Entfernen mit infacmd isp [719](#)
- Erstellen [502](#)
- Zuweisen zum Metadata Manager-Dienst [404](#)

## Integrationsdienst-Prozess

- Abrufen von Eigenschaften [578](#)
- Aktualisieren der Optionen für [810](#)

## Interactive Data Preparation Service

- creating [304](#)
- updating [309](#)

## Interaktiver Modus für pmcmd

- Festlegen von Standardwerten [1394](#)
- Verbinden [1394](#)

## J

## Jobs

- abbrechen [970](#)
- Bereinigen [989](#)

## Jobs des Datenintegrationsdiensts löschen [989](#)

## K

## KillUserConnection (pmrep)

- Beschreibung [1489](#)

## Knoten

- Abrufen des Namens von [573](#)
- Aktualisieren [794](#)
- Aktualisieren der Gateway mit infasetup [817](#), [1367](#), [1386](#)
- Aktualisieren der Rolle [796](#)
- Aktualisieren des Arbeitsknotens mit infasetup [1379](#)
- Auflisten mit infacmd isp [660](#)
- Auflisten von allen in einer Domäne [650](#)
- Auflisten von Optionen mit infacmd isp [645](#)
- Auflisten von Rollen [648](#)
- Definieren des Gateways mit infasetup [1342](#)
- Definieren von Arbeitsknoten mit infasetup [1349](#)
- Entfernen aus Domänen [710](#)
- Hinzufügen von Ressourcen [388](#)
- Hinzufügen zu Domänen [376](#)
- Pingen [679](#)
- Trennen von Domänen mit infacmd isp [762](#)
- Wechseln von Arbeits- zu Gateway-Knoten mit infacmd [745](#)
- Wechseln von Gateway- zu Arbeitsknoten mit infacmd isp [747](#)

## konfigurieren

- Befehlszeilendienstprogramme [33](#)

## Konnektivität

- Verbindungsstring, Beispiele [1443](#)

## L

## LDAP-Authentifizierung

- Einrichten mit infacmd isp [371](#), [380](#), [768](#), [781](#)

## LDAP-Severkonfiguration

- Aktualisieren mit infacmd isp [739](#)
- Auflisten mit infacmd isp [654](#)

## LDAP-Verbindung

- Auflisten mit infacmd isp [604](#), [607](#), [622](#), [640](#), [693](#), [706](#)

## Links

- Hinzufügen zu Domänen [374](#)

## List (infacmd ps) [1021](#)

## listActiveWorkflowInstances

- infacmd wfs [1251](#)

## ListAlertUsers (infacmd isp)

- Beschreibung [602](#)

## listAllCustomLDAPTypes (infacmd isp)

- Beschreibung [604](#)

## ListAllGroups (infacmd isp)

- Beschreibung [605](#)

## listAllLDAPConnectivity (infacmd isp)

- Beschreibung [607](#)

## ListAllProfiles (infacmd ps) [1023](#)

## ListAllRoles (infacmd isp)

- Beschreibung [608](#)

## ListAllUsers (infacmd isp)

- Beschreibung [610](#)

## ListAllUsers (pmrep)

- description [1490](#)

## ListApplicationObjectPermissions (infacmd dis) [191](#)

## ListApplicationObjects (infacmd dis) [193](#)

## ListApplicationOptions (infacmd dis) [195](#)

## ListApplicationPermissions (infacmd dis) [197](#)

## ListApplications (infacmd dis) [199](#)

## listAssociatedConnections (infacmd cluster) [113](#)

## ListBackupFiles (infacmd mrs) [913](#)

- ListCheckedOutObjects (infacmd mrs) [915](#)
- listClusters (infacmd ccps) [97](#)
- ListColumnOptions (infacmd sql) [1169](#)
- ListComputeNodeAttributes (infacmd rms) [1114](#)
- ListComputeOptions (infacmd dis) [200](#), [264](#)
- listConfigurationGroupPermissions (infacmd cluster) [115](#)
- listConfigurationProperties (infacmd cluster) [118](#)
- listConfigurations (infacmd cluster) [120](#)
- listConfigurationSets (infacmd cluster) [117](#)
- listConfigurationUserPermissions (infacmd cluster) [122](#)
- ListConnectionOptions (infacmd isp)
  - Beschreibung [611](#), [621](#)
- ListConnectionPermissionByUser (infacmd isp) [617](#)
- ListConnectionPermissions (infacmd isp) [613](#)
- ListConnectionPermissionsByGroup (infacmd isp)
  - Beschreibung [615](#)
- ListConnections (infacmd isp)
  - Beschreibung [619](#)
- ListConnections (pmrep)
  - Beschreibung [1489](#)
- listCustomLDAPType (infacmd isp)
  - Beschreibung [622](#)
- ListDataObjectOptions (infacmd dis) [202](#)
- ListDefaultOSProfiles (infacmd isp) [624](#)
- ListDomainLinks (infacmd isp)
  - Beschreibung [628](#)
- ListDomainOptions (infacmd isp)
  - Beschreibung [630](#)
- ListFolders (infacmd isp)
  - Beschreibung [631](#)
- ListFolders (infacmd mrs) [917](#)
- listGlossary (infacmd bg) [89](#)
- ListGridNodes (infacmd isp)
  - Beschreibung [633](#)
- ListGroupPermissions (infacmd isp) [634](#)
- ListGroupPrivileges (infacmd isp)
  - Beschreibung [636](#)
- ListGroupsForUser (infacmd isp) [638](#)
- ListLDAPConnectivity (infacmd isp)
  - Beschreibung [640](#)
- ListLicenses (infacmd isp)
  - Beschreibung [642](#)
- ListLockedObjects (infacmd mrs) [919](#)
- listMappingEngines (infacmd dis) [204](#)
- listMappingEngines (infacmd mrs) [921](#)
- listMappingOptions (infacmd ms) [981](#)
- listMappingPersistedOutputs
  - infacmd wfs [1253](#)
- ListMappings (infacmd ms) [987](#)
- listMonitoringOptions (infacmd isp) [644](#)
- ListNodeOptions (infacmd isp)
  - Beschreibung [645](#)
- ListNodeResources (infacmd isp)
  - Beschreibung [647](#)
- ListNodeRoles (infacmd isp) [648](#)
- ListNodes (infacmd isp)
  - Beschreibung [650](#)
- ListObjectDependencies (pmrep)
  - description [1490](#)
- ListObjects (pmrep)
  - Auflisten von Ordnern [1497](#)
  - Beschreibung [1492](#)
  - transformation types [1494](#)
- ListOperationOptions
  - infacmd ws [1279](#)
- ListOSProfiles (infacmd isp)
  - Beschreibung [652](#)
- ListParameterSetObjects (infacmd dis) [209](#)

- ListParameterSets (infacmd dis) [211](#)
- listPatchNames
  - infacmd dis [212](#)
- listPermissionOnProject (infacmd mrs) [923](#)
- ListPlugins (infacmd) [65](#)
- listProcessProperties
  - infacmd roh [1101](#)
- ListProjects (infacmd mrs) [925](#)
- ListRepositoryLDAPConfiguration (infacmd isp)
  - Beschreibung [654](#)
- ListRolePrivileges (infacmd isp)
  - Beschreibung [655](#)
- ListSchedule (infacmd sch) [1138](#)
- ListSecurityDomains (infacmd)
  - Beschreibung [657](#)
- ListSequenceObjectProperties (infacmd dis) [214](#)
- ListSequenceObjects (infacmd dis) [216](#)
- ListServiceLevels (infacmd isp)
  - Beschreibung [659](#)
- ListServiceNodes (infacmd isp)
  - Beschreibung [660](#)
- listServiceOptions
  - infacmd roh [1106](#)
- ListServiceOptions (infacmd as) [73](#)
- ListServiceOptions (infacmd cms) [139](#)
- ListServiceOptions (infacmd mas) [853](#)
- ListServiceOptions (infacmd mrs) [927](#)
- ListServiceOptions (infacmd rms) [1116](#)
- ListServiceOptions (infacmd sch) [1140](#)
- ListServiceOptions (infacmd search) [1160](#)
- ListServicePrivileges (infacmd isp)
  - Beschreibung [662](#)
- listServiceProcessOptions
  - infacmd roh [1104](#)
- ListServiceProcessOptions (infacmd as) [73](#)
- ListServiceProcessOptions (infacmd cms) [141](#)
- ListServiceProcessOptions (infacmd dis) [217](#)
- ListServiceProcessOptions (infacmd mas) [855](#)
- ListServiceProcessOptions (infacmd mrs) [929](#)
- ListServiceProcessOptions (infacmd sch) [1141](#)
- ListServiceProcessOptions (infacmd search) [1162](#)
- ListServices (infacmd isp)
  - Beschreibung [664](#)
- ListSMTPOptions (infacmd isp) [666](#)
- listSpecs (infacmd mi) [876](#)
- ListSQLDataServiceOptions (infacmd sql) [1173](#)
- ListSQLDataServicePermissions (infacmd sql) [1175](#)
- ListSQLDataServices (infacmd sql) [1176](#)
- ListStoredProcedurePermissions (infacmd sql) [1178](#)
- ListTableOptions (infacmd sql) [1180](#)
- ListTablePermissions (infacmd sql) [1171](#), [1182](#)
- ListTablesBySess (pmrep)
  - Beschreibung [1498](#)
- ListTaskListener (infacmd pwx) [1080](#)
- listTasks
  - infacmd wfs [1255](#)
- ListUserConnections (pmrep)
  - Beschreibung [1499](#)
- ListUserPermissions (infacmd isp) [668](#)
- ListUserPrivileges (infacmd isp)
  - Beschreibung [670](#)
- ListWeakPasswordUsers (infacmd) [672](#)
- ListWebServiceOptions
  - infacmd ws [1283](#)
- ListWebServicePermissions
  - infacmd ws [1285](#)
- ListWebServices
  - infacmd ws [1287](#)

- listWorkflowParameters
  - infacmd wfs [1258](#)
- listWorkflows
  - infacmd wfs [1261](#)
- Lizenzen
  - Aktualisieren mit infacmd isp [784](#)
  - Anzeigen mit infacmd isp [742](#)
  - Aufheben der Zuweisung mit infacmd [754](#)
  - Auflisten mit infacmd isp [642](#)
  - Auflisten von zugewiesenen Diensten [400](#)
  - Entfernen mit infacmd isp [708](#)
  - Hinzufügen zu Domänen [383](#)
- Logische Datenobjekte
  - Bereinigen des Caches [219](#)
  - Optionen für infacmd [268](#)
- Logische Operatoren
  - query [293](#)
- logischer Datenobjekt-Cache
  - Aktualisierung stoppen für [161](#)
- Lokale Parameterdateien
  - Verwenden mit pmcmd StartWorkflow [1428](#)

## M

- ManageGroupPermissionOnProject (infacmd mrs) [931](#)
- ManageUserPermissionOnProject (infacmd mrs) [933](#)
- Mapping
  - Einrichten von Berechtigungen [237](#)
- Mapping-Status
  - Zugreifen mit infacmd ms [977](#)
- Massenerfassung
  - Ausführungsstatistik [872](#)
- Massenerfassungsdienst
  - erstellen [866](#)
- Massenerfassungsspezifikation
  - abbrechen [864](#)
- MassUpdate (pmrep)
  - Beschreibung [1499](#)
- Metadata Manager-Dienst
  - Aktualisieren von Eigenschaften für [786](#)
  - Erstellen in einer Domäne [513](#)
- Metadata Manager-Dienstprogramme
  - Installation [32](#)
  - konfigurieren [34](#)
  - Sicherheitskonfiguration [35](#)
- Metadaten-Zugriffsdienst
  - Auflisten von Eigenschaften für [853](#)
  - erstellen [849](#)
  - Konfigurieren von Eigenschaften für [857](#)
- Metadaten-Zugriffsdienst-Optionen
  - infacmd-Syntax [859](#)
- Metadaten-Zugriffsdienst-Prozess
  - Auflisten von Eigenschaften für [855](#)
  - Konfigurieren von Eigenschaften für [860](#)
- Microsoft Azure Blob Storage-Verbindung
  - infacmd-Eigenschaften [469](#)
- Microsoft Azure Data Lake Storage Gen1-Verbindung
  - infacmd-Eigenschaften [470](#)
- Microsoft Azure Data Lake Storage Gen2-Verbindung
  - infacmd-Eigenschaften [471](#)
- Microsoft Azure SQL Data Warehouse-Verbindung
  - infacmd-Eigenschaften [471](#)
- Microsoft SQL Server
  - Verbindungsstring-Syntax [1443](#)
- MigrateEncryptionKey (infasetup)
  - Beschreibung [1358](#)
- migrateProfileResults (infacmd ps) [1024](#)

- migrateScorecards (infacmd ps) [1026](#)
- migrateUsers
  - infacmd isp [674](#)
- Modellrepository
  - Aktualisiert die Statistik des Modellrepository-Diensts [963](#)
  - Aktualisiert Dienstprozessoptionen für den Modellrepository-Dienst [961](#)
  - Aktualisiert Optionen für den Modellrepository-Dienst [954](#)
  - Auflisten von ausgecheckten Objekten in [915](#)
  - Auflisten von Berechtigungen für verschiedene Projekte [923](#)
  - Auflisten von Dateien im Backup-Ordner [913](#)
  - Auflisten von gesperrten Objekten in [919](#)
  - Auflisten von Ordnern im Repository des Modellrepository-Diensts [917](#)
  - Auflisten von Projekten im Repository des Modellrepository-Dienst [925](#)
  - Einchecken von Objekten [886](#)
  - Entsperren eines Objekts in [952](#)
  - Erstellt die Objektabhängigkeitsgrafik neu. [938](#)
  - Listet Optionen für den Modellrepository-Dienst auf [927](#)
  - Löschen des Inhalts [899](#)
  - Neuzuweisung eines ausgecheckten Objekts in [936](#)
  - Neuzuweisung eines gesperrten Objekts in [936](#)
  - Sichern von Inhalten in einer Datei [884](#)
  - Upgraden von Inhalten des Modellrepository-Dienst [965](#)
  - Wiederherstellen der Inhalte [944](#)
  - Wiederherstellen von ausgecheckten Objekten in [946](#), [950](#)
- Modellrepository-Dienst
  - auflisten [921](#)
  - Auflisten [929](#)
  - Erstellen [894](#)
  - Erstellen von Repository-Inhalt [888](#)
- Modellrepository-Objekte
  - Exportieren [357](#)
  - Wiederverwendung eines Berichtsobjekts [363](#)
- ModifyFolder (pmrep)
  - Beschreibung [1505](#)
- MoveFolder (infacmd isp)
  - Beschreibung [675](#)
- MoveObject (infacmd isp)
  - Beschreibung [677](#)

## N

- Nachträgliche E-Mail für die Sitzung
  - Aktualisieren von Adressen mit pmrep [1528](#)
- Notify (pmrep)
  - Beschreibung [1507](#)

## O

- ObjectExport (pmrep)
  - Beschreibung [1507](#)
- ObjectImport (pmrep)
  - Beschreibung [1509](#)
- Objekte
  - Bereitstellen in einer Archivdatei [1224](#)
  - Einchecken [1455](#)
  - Entfernen von Benutzerberechtigungen [726](#)
  - Exportieren [1507](#)
  - Exportieren in Objektexportdatei [1226](#)
  - Importieren [1509](#)
  - Importieren aus Objektexportdatei [1230](#)
  - Löschen [1475](#)
  - Zuweisen von Benutzerberechtigungen [414](#)

- Objektimport-Steuerdatei
  - Beschreibung [1553](#)
- Olson-Zeitzone
  - gültige Werte [1133](#)
- Optimierungsebene
  - Aktualisieren [998](#)
- optimization level
  - Aktualisieren [1000](#)
- Optionen des Datenintegrationsdiensts
  - infacmd-Syntax [273](#)
- Optionen des Ressourcenmanager-Diensts
  - infacmd-Syntax [1121](#)
- Optionen des Scheduler-Diensts
  - infacmd-Syntax [1151](#), [1153](#)
- Oracle
  - Verbindungsoptionen für [480](#)
  - Verbindungsstring-Syntax [1443](#)
- Ordner
  - Aktualisieren der Beschreibung mit infacmd isp [773](#)
  - Ändern [1505](#)
  - Auflisten mit infacmd isp [631](#)
  - Bereitstellen [1478](#)
  - Entfernen mit infacmd isp [697](#)
  - Erstellen in einer Domäne [496](#)
  - Löschen [1474](#)
  - Verschieben mit infacmd isp [675](#)
  - Verschieben von Objekten zwischen Ordnern mit infacmd isp [677](#)
- Ordnerpfad
  - Vergleichsoperatoren [292](#)
- OVERRIDEFOLDER
  - Beispielsteuerdatei [1572](#)

## P

- Parameterdateien
  - Verwenden mit pmcmd StartTask [1424](#)
  - Verwenden mit pmcmd StartWorkflow [1428](#)
- passwords
  - encrypting [61](#)
- Passwörter
  - Zurücksetzen von Benutzerpasswörtern mit infacmd isp [733](#)
- Patch
  - Anwendung [1235](#)
  - Inkrementelle Anwendung [1235](#)
- PauseAll (infacmd sch) [1142](#)
- PauseSchedule (infacmd sch) [1143](#)
- Persistente Eingabedatei
  - Erstellen mit pmrep [1551](#)
- ping
  - Dienst [680](#)
  - Domäne [680](#)
  - Knoten [680](#)
- Ping (infacmd isp)
  - Beschreibung [679](#)
- pingservice (pmcmd)
  - Beschreibung [1415](#)
- Plug-Ins
  - XML-Vorlagen [1516](#)
- pmcmd
  - Arbeitsabläufe, Abbrechen [1399](#)
  - Arbeitsabläufe, Abrufen von Informationen über [1404](#), [1411](#)
  - Arbeitsabläufe, Beenden [1431](#)
  - Arbeitsabläufe, Entfernen aus einem Zeitplan [1433](#)
  - Arbeitsabläufe, Ermitteln der Ausführung [1437](#)
  - Arbeitsabläufe, Planen [1418](#)
  - Arbeitsabläufe, Starten [1425](#)
  - Arbeitsabläufe, Wiederherstellen [1416](#)

- pmcmd (Fortsetzung)
  - Aufgaben, Abbrechen [1397](#)
  - Aufgaben, Abrufen von Informationen über [1404](#), [1409](#)
  - Aufgaben, Abschließen vor der Zurückgabe der Eingabeaufforderung [1435](#)
  - Aufgaben, Anhalten [1429](#)
  - Aufgaben, Starten [1421](#)
  - Ausführen in einer Domäne für verschiedene Versionen [1392](#)
  - Befehlszeilenmodus [1392](#)
  - Integration Service, Anpingen [1415](#)
  - Integration Service, Trennen von [1402](#)
  - Integration Service, Verbinden mit [1401](#)
  - Interaktiver Modus [1394](#)
  - Interaktiver Modus, Beenden [1403](#)
  - nowait-Modus, Einrichten [1420](#)
  - Ordner, Festlegen für die Ausführung von Befehlen [1420](#)
  - Ordner, Kennzeichnen als Nicht-Standardordner [1435](#)
  - Parameterdateien [1424](#), [1428](#)
  - PowerCenter Integration Service, Abrufen der Eigenschaften [1406](#)
  - Rückgabewerte [1393](#)
  - Service-Einstellungen, Abrufen [1421](#)
  - Sitzungen, Abrufen von Informationen über [1403](#)
  - Sitzungsstatistiken, Abrufen [1407](#)
  - Skriptdateien [1396](#)
  - Version, Anzeigen [1435](#)
  - wait-Modus, Einrichten [1421](#)
- pmpasswd
  - encrypting passwords [61](#)
  - syntax [61](#)
- pmrep
  - Abfragen, Ausführen [1480](#)
  - Ausführen in einer Domäne für verschiedene Versionen [1442](#)
  - Ausgecheckte Objekte, Auflisten [1482](#)
  - Befehlszeilenmodus [1442](#)
  - Benachrichtigungsmeldungen, Senden [1507](#)
  - Benutzereigenschaften, Bearbeiten [1480](#)
  - Benutzerverbindungen, Auflisten [1499](#)
  - Benutzerverbindungen, Beenden [1489](#)
  - Berechtigung, Zuweisen [1452](#)
  - Berechtigungen, Entfernen [1518](#)
  - Bereitstellung, Rollback [1518](#)
  - Bereitstellungs-Steuerdatei-Parameter [1566](#)
  - Bereitstellungsgruppen, Bereitstellen [1477](#)
  - Bereitstellungsgruppen, Erstellen [1464](#)
  - Bereitstellungsgruppen, Hinzufügen von Objekten zu [1447](#)
  - Bereitstellungsgruppen, Löschen [1474](#)
  - Bereitstellungsgruppen, Löschen von Objekten aus [1456](#)
  - Beschriftungen, Anwenden [1449](#)
  - Beschriftungen, Erstellen [1466](#)
  - Beschriftungen, Löschen [1475](#)
  - Checkouts, Rückgängig machen [1522](#)
  - Deinstallieren des ABAP-Programms [1533](#)
  - E-Mail-Adressen, Aktualisieren [1528](#)
  - Generieren des ABAP-Programms [1484](#)
  - Gruppen, Erstellen [1466](#)
  - hilfe [1486](#)
  - Installieren des ABAP-Programms [1486](#)
  - Interaktiver Modus [1442](#)
  - Interaktiver Modus, Beenden [1482](#)
  - Namenspräfixe von Target-Tabellen, Aktualisieren [1532](#)
  - object dependencies, listing [1490](#)
  - Objekte, Ändern des Eigentümers [1455](#)
  - Objekte, Auflisten [1492](#)
  - Objekte, Einchecken [1455](#)
  - Objekte, Exportieren [1507](#)
  - Objekte, Importieren [1509](#)
  - Objekte, Löschen [1475](#)
  - Objekte, Validieren [1535](#)



## pmrep (Fortsetzung)

- Objektversionen, Bereinigen [1510](#)
- Ordner, Ändern von Eigenschaften [1505](#)
- Ordner, Auflisten [1497](#)
- Ordner, Bereitstellen [1478](#)
- Ordner, Erstellen [1464](#)
- Ordner, Löschen [1474](#)
- Ordneigenschaften, Ändern [1505](#)
- Persistente Eingabedateien, Erstellen [1551](#)
- Plug-Ins, Aufheben der Registrierung [1524](#)
- Plug-Ins, Registrieren [1515](#)
- PowerCenter-Integrationsdienst, zuweisen [1451](#)
- Protokolle, Löschen [1521](#)
- Repositories, Aufheben der Registrierung [1523](#)
- Repositories, Erstellen [1459](#)
- Repositories, Löschen [1472](#)
- Repositories, Registrieren [1513](#)
- Repositories, Sichern [1454](#)
- Repositories, Wiederherstellen [1517](#)
- Repository-Statistiken, Aktualisieren [1531](#)
- Repository-Verbindungsdatei, Angeben [58](#)
- Repositorys, Verbinden mit [1457](#)
- Ressourcen, Bereinigen [1456](#)
- Sequenzwerte, Aktualisieren [1529](#)
- Skriptdateien [1444](#)
- Skripts, Ausführen [1519](#)
- Steuerparameter für Objektimport [1554](#)
- Tabellen, Auflisten nach Sitzung [1498](#)
- Tabelleneigentümernamen, Aktualisieren [1530](#)
- Übersicht [1442](#)
- users, listing [1490](#)
- Verbindungen, Aktualisieren [1526](#)
- Verbindungen, Auflisten [1489](#)
- Verbindungen, Erstellen [1460](#)
- Verbindungen, Löschen [1473](#)
- Verbindungsdetails, Auflisten [1484](#)
- Verbindungsinformationen, Anzeigen [1520](#)
- Verbindungsname, Ändern [1520](#)
- Versionsinformationen, Anzeigen [1537](#)
- PopulateVCS (infacmd mrs) [935](#)
- PowerCenter IntegrationService
  - Zuweisen mit pmrep [1451](#)
- PowerCenter-Dienstprogramme
  - Installation [32](#)
  - konfigurieren [33](#)
  - Sicherheitskonfiguration [35](#)
- PowerCenter-Ressourcen
  - Aktivieren [553](#)
  - Deaktivieren [542](#)
- PowerExchange-Listenerdienst
  - Aktualisieren von Eigenschaften [1092](#)
  - Anhalten [1040](#)
  - Anzeigen von Überwachungsstatistiken für den Listenerdienst und dessen Aufgaben [1071](#)
  - Auflisten von Aufgaben [1080](#)
  - Beenden von Aufgaben [1086](#)
  - erstellen [1049](#)
  - Erzwingen des Abbruchs [1037](#)
- PowerExchange-Protokollierungsdienst
  - Aktualisieren von Eigenschaften [1096](#)
  - Anzeigen aller Nachrichten [1056](#)
  - Anzeigen der Anzahl an verarbeiteten Änderungsdatensätzen [1068](#)
  - Anzeigen der Speichernutzung [1065](#)
  - Anzeigen des Status der Writer-Unteraufgabe [1074](#)
  - Anzeigen von CPU-Informationen [1059](#)
  - Anzeigen von Ereignissen [1062](#)
  - erstellen [1051](#)
  - Herunterfahren [1083](#)

## PowerExchange-Protokollierungsdienst (Fortsetzung)

- Starten des Protokollierungszyklus [1043](#)
- Wechseln zu einem neuen Satz an Logdateien. [1077](#)
- PrintSPNAndKeytabNames (infacmd isp) [682](#)
- Profilaufgaben
  - Abrufen des Status [1017](#), [1034](#)
- Profile
  - Auflisten von Ergebnissen für [1021](#)
  - Ausführen [1013](#)
  - Bereinigen von Ergebnissen für [1028](#)
  - Erkennen von Ergebnissen für [1010](#)
  - Erkennen von Tabellen für [1030](#)
- Profiling Warehouse-Inhalte
  - Entfernen [1011](#)
- Profilmodell
  - Abrufen des Status [1019](#)
  - ausführen [1015](#)
  - Wird abgebrochen [1006](#)
- Protokollereignisse
  - Bereinigen mit infacmd isp [683](#)
  - Trunkieren mit pmrep [1521](#)
- Provider-URL angeben
  - Abrufen [575](#)
  - festlegen [1376](#)
- pruneOldInstances
  - infacmd wfs [1263](#)
- Purge (infacmd ps) [1028](#)
- purgeauditevents (infacmd edp) [320](#)
- purgeDatabaseWorkTabless (infacmd dm) [989](#)
- PurgeDataObjectCache (infacmd dis) [219](#)
- PurgeLog (infacmd isp)
  - Beschreibung [683](#)
- purgeOrphanResults (infacmd ps) [1030](#)
- PurgeResultSetCache (infacmd dis) [221](#)
- PurgeTableCache (infacmd sql) [1183](#)
- PurgeVersion (pmrep)
  - Beschreibung [1510](#)

## Q

- query
  - Abfrageparameter [293](#)
  - Abfragestruktur [295](#)
  - infacmd dis [290](#)
  - Logische Operatoren [293](#)
  - Vergleichsoperatoren [291](#)
  - Where-Klausel [295](#)
- queryDesignTimeObjects
  - infacmd dis [223](#)
- queryRunTimeObjects
  - infacmd dis [225](#)

## R

- reassignCheckedOutObject (infacmd mrs) [936](#)
- rebuildDependencyGraph (infacmd mrs) [938](#)
- recoverWorkflow
  - infacmd wfs [1265](#)
- recoverworkflow (pmcmd)
  - Beschreibung [1416](#)
- Referenztabellen
  - Exportieren [1124](#)
  - Importieren in Modellrepositorys [1127](#)
- refreshConfiguration (infacmd cluster) [123](#)
- RefreshDataObjectCache (infacmd dis) [227](#)
- RefreshTableCache (infacmd sql) [1185](#)

- Register (pmrep)
  - Beschreibung [1513](#)
- RegisterPlugin (pmrep)
  - Beschreibung [1515](#)
- Registrieren
  - Plug-In mit pmrep [1515](#)
  - Sicherheitsmodul mit pmrep [1516](#)
- releaseTask
  - infacmd wfs [1267](#)
- RemoveAlertUser (infacmd isp)
  - Beschreibung [687](#)
- RemoveConnection (infacmd isp)
  - Beschreibung [689](#)
- RemoveConnectionPermissions (infacmd isp)
  - Beschreibung [691](#)
- removeCustomLDAPType (infacmd isp)
  - Beschreibung [693](#)
- RemoveDomainLink (infacmd isp)
  - Beschreibung [695](#)
- RemoveFolder (infacmd isp)
  - Beschreibung [697](#)
- RemoveGrid (infacmd isp)
  - Beschreibung [699](#)
- RemoveGroup (infacmd isp)
  - Beschreibung [700](#)
- RemoveGroupPermission (infacmd isp) [702](#)
- RemoveGroupPrivilege (infacmd isp)
  - Beschreibung [704](#)
- removeLDAPConnectivity (infacmd isp)
  - Beschreibung [706](#)
- RemoveLicense (infacmd isp)
  - Beschreibung [708](#)
- RemoveNode (infacmd isp)
  - Beschreibung [710](#)
- RemoveNodeResource (infacmd isp)
  - Beschreibung [711](#)
- RemoveOSProfile (infacmd isp)
  - Beschreibung [713](#)
- RemoveRole (infacmd isp)
  - Beschreibung [715](#)
- RemoveRolePrivilege (infacmd isp)
  - Beschreibung [717](#)
- RemoveService (infacmd cms) [145](#)
- RemoveService (infacmd isp)
  - Beschreibung [719](#)
- RemoveServiceLevel (infacmd isp)
  - Beschreibung [721](#)
- RemoveUser (infacmd isp)
  - Beschreibung [723](#)
- RemoveUserFromGroup (infacmd isp)
  - Beschreibung [725](#)
- RemoveUserPermission (infacmd isp) [726](#)
- RemoveUserPrivilege (infacmd isp)
  - Beschreibung [729](#)
- RenameApplication (infacmd dis) [228](#)
- RenameConnection (infacmd isp) [731](#)
- RenameFolder (infacmd mrs) [940](#)
- RenameSQLDataService (infacmd sql) [1187](#)
- RenameWebService
  - infacmd ws [1289](#)
- replaceAllTag
  - infacmd dis [256](#)
- Repositories
  - Aufheben der Registrierung [1523](#)
  - Löschen von Details aus [1521](#)
  - Registrieren [1513](#)
  - Sichern mit pmrep [1454](#)

- Repository-Dienst
  - Aktualisieren mit infacmd isp [802](#)
  - Entfernen mit infacmd isp [719](#)
  - Erstellen in einer Domäne [522](#)
- Repositorys
  - Erstellen von relationalen [1460](#)
  - Verbinden mit pmrep [1457](#)
- ResetPassword (infacmd isp)
  - Beschreibung [733](#)
- Ressourcen
  - Anzeigen mit infacmd isp [647](#)
  - Entfernen mit infacmd isp [711](#)
  - Exportieren in Objektexportdatei [1228](#)
- Ressourcenmanager-Dienst
  - Auflisten von Eigenschaften für [1116](#)
  - Konfigurieren von Eigenschaften für [1119](#)
- restartMapping (infacmd mi) [877](#)
- Restore (pmrep)
  - Beschreibung [1517](#)
- RestoreApplication (infacmd dis) [233](#)
- RestoreContents (infacmd mrs) [944](#)
- RestoreDomain (infasetup)
  - Beschreibung [1359](#)
- restoreMitKerberosLinkage (infasetup)
  - Beschreibung [1362](#)
- ResumeAll (infacmd sch) [1144](#)
- ResumeSchedule (infacmd sch) [1145](#)
- resyncData (infacmd cms) [147](#)
- RevertObject (infacmd mrs) [946](#), [950](#)
- revive\_Scorecards (infacmd ps) [1032](#)
- RmPrivilege (pmrep)
  - Beschreibung [1518](#)
- RollbackDeployment (pmrep)
  - Beschreibung [1518](#)
- Rollen
  - Auflisten mit infacmd isp [608](#)
  - Entfernen aus einer Gruppe mit infacmd isp [756](#)
  - Entfernen mit infacmd isp [715](#)
  - Entfernen von einem Benutzer mit infacmd isp [758](#)
  - Erstellen in einer Domäne [527](#)
  - Exportieren mit infacmd isp [560](#)
  - Importieren mit infacmd isp [595](#)
  - Zuweisen zu einem Benutzer mit infacmd isp [410](#)
- Rückgabewerte
  - infacmd [67](#)
  - infasetup [1328](#)
  - pmcmd [1393](#)
- Run (pmrep)
  - Beschreibung [1519](#)
- RunCPUProfile (infacmd isp)
  - Beschreibung [735](#)
- RunMapping
  - infacmd ms [991](#)
- runSpec
  - infacmd mi [879](#)

## S

- SAP BW-Dienst
  - Aktualisieren mit infacmd isp [807](#)
  - Erstellen in einer Domäne [529](#)
- scheduleworkflow (pmcmd)
  - Beschreibung [1418](#)
- Schemadateien
  - infacmd-Steuerdateien [1309](#)
- Scorecards
  - Auflisten von Ergebnissen für [1021](#)



## Scorecards (Fortsetzung)

- Ausführen [1013](#)
- Bereinigen von Ergebnissen für [1028](#)
- Migrieren [1026](#)

## SEQ

- infacmd-Verbindungsoptionen [486](#)
- SetApplicationObjectPermissions (infacmd dis) [237](#)
- SetApplicationPermissions (infacmd dis) [234](#)
- SetColumnPermissions (infacmd sql) [1189](#)
- SetComputeNodeAttributes (infacmd rms) [1117](#)
- setConfigurationPermissions (infacmd cluster) [125](#)
- SetConnectionPermissions (infacmd isp) [737](#)
- SetFolder (pmcmd)
  - Beschreibung [1420](#)
- setMappingPersistedOutputs
  - infacmd wfs [1269](#)
- SetNoWait (pmcmd)
  - Beschreibung [1420](#)
- SetOperationPermissions
  - infacmd ws [1291](#)
- SetRepositoryLDAPConfiguration (infacmd isp)
  - Beschreibung [739](#)
- SetSequenceState (infacmd dis) [241](#)
- SetSQLDataServicePermissions (infacmd sql) [1191](#)
- SetStoredProcedurePermissions (infacmd sql) [1194](#)
- SetTablePermissions (infacmd sql) [1197](#)
- SetWait (pmcmd)
  - Beschreibung [1421](#)
- SetWebServicePermissions
  - infacmd ws [1294](#)
- ShowConnectionInfo (pmrep)
  - Beschreibung [1520](#)
- ShowLicense (infacmd isp)
  - Beschreibung [742](#)
- ShowSettings (pmcmd)
  - Beschreibung [1421](#)
- ShutDownLogger (infacmd pwx) [1083](#)
- ShutdownNode (infacmd isp)
  - Beschreibung [744](#)
- Sicherheitsdomänen
  - Auflisten mit infacmd [657](#)
- Sitzungen
  - Abrufen von Protokollereignissen [584](#)
- Skriptdateien
  - running [1519](#)
  - Verwenden für pmrep-Befehle [1444](#)
- Spalte
  - Optionen für infacmd [1205](#)
- Spalte für virtuelle Tabelle
  - Einrichten von Berechtigungen [1189](#)
- Spalten
  - Auflisten von Eigenschaften für [1169](#)
- spec
  - Bereitstellen in einer Archivdatei [871](#)
- Spezifikationen, die einem Datenintegrationsdienst bereitgestellt werden
  - wird ausgeführt [879](#)
- Spezifikationsstatus
  - Zugriff mit infacmd mi [874](#)
- SQL-Datendienst
  - Aktualisieren der Optionen für [1206](#)
  - Anhalten [1201](#)
  - Auflisten für einen Datenintegrationsdienst [1176](#)
  - Auflisten von Berechtigungen [1175](#)
  - Auflisten von Eigenschaften für [1173](#)
  - Einrichten von Berechtigungen [1191](#)
  - Optionen für infacmd [1207](#)
  - Starten [1199](#)

## SQL-Datendienst (Fortsetzung)

- Umbenennen [1187](#)
- StartApplication (infacmd dis) [244](#)
- StartSQLDataService (infacmd sql) [1199](#)
- startTask
  - infacmd wfs [1272](#)
- StartTask (pmcmd)
  - Beschreibung [1421](#)
  - Verwenden einer Parameterdatei [1424](#)
- StartWebService
  - infacmd ws [1297](#)
- startWorkflow
  - infacmd wfs [1273](#)
- StartWorkflow (pmcmd)
  - Beschreibung [1425](#)
  - Verwenden einer Parameterdatei [1428](#)
- Statistiken
  - Aktualisieren des Repository [1531](#)
- Steuerdatei
  - Bereitstellung [1564](#)
  - ObjectImport XML-Beispiel [1557](#)
  - Objektimport [1553](#)
- Steuerdateien
  - Beispiele für Domänenobjekte [1324](#)
  - Beispiele für Model Repository-Objekte [1325](#)
  - Benennungskonventionen [1310](#)
  - infacmd [1309](#)
  - Parameter für Domänenobjekte [1311](#), [1316](#)
  - Parameter für Modellrepository-Objekte [1312](#), [1318](#)
  - Regeln und Richtlinien [1323](#)
  - Schemadateien [1309](#)
- StopApplication (infacmd dis) [246](#)
- stopBlazeService (infacmd dis) [248](#)
- StopSQLDataService (infacmd sql) [1201](#)
- StopTask (pmcmd)
  - Beschreibung [1429](#)
- StopTaskListener (infacmd pwx) [1086](#)
- StopWebService
  - infacmd ws [1299](#)
- StopWorkflow (pmcmd)
  - Beschreibung [1431](#)
- Suchdienst
  - Auflisten von Eigenschaften für [1160](#)
  - erstellen [1157](#)
  - Konfigurieren von Eigenschaften für [1164](#)
- Suchdienstprozess
  - Auflisten von Eigenschaften für [1162](#)
  - Konfigurieren von Eigenschaften für [1166](#)
- SwitchConnection (pmrep)
  - Beschreibung [1520](#)
- SwitchToGatewayNode (infacmd)
  - Beschreibung [745](#)
- SwitchToKerberosMode (infasetup)
  - beschreibung [1363](#)
- SwitchToWorkerNode (infacmd isp)
  - Beschreibung [747](#)
- synchronizeProfile (infacmd ps) [1034](#)
- SyncSecurityDomains (infacmd isp) [749](#)
- syntax
  - infacmd-Optionen des Ressourcenmanager-Diensts [1121](#)
- Syntax
  - Befehlszeilenprogramme [38](#)
  - infacmd-Optionen des Datenintegrationsdiensts [273](#)
  - infacmd-Optionen des Scheduler-Diensts [1151](#), [1153](#)
  - Metadaten-Zugriffsdienst, infacmd-Optionen [859](#)

## T

Tabelleneigentümername  
Aktualisieren mit pmrep [1530](#)  
Tag  
infacmd dis [251](#)  
TDM-Dienst  
deaktivieren [1221](#)  
Test Data Manager-Dienst  
in einer Domäne erstellen [1212](#), [1218](#)  
TruncateLog (pmrep)  
Beschreibung [1521](#)

## U

Umgebungsvariablen  
ICMD\_JAVA\_OPTS [45](#)  
INFA\_CLIENT\_RESILIENCE\_TIMEOUT [46](#)  
INFA\_CODEPAGENAME [47](#)  
INFA\_DEFAULT\_DATABASE\_PASSWORD [47](#)  
INFA\_DEFAULT\_DB\_TRUSTSTORE\_PASSWORD [49](#)  
INFA\_DEFAULT\_DOMAIN [50](#)  
INFA\_DEFAULT\_DOMAIN\_PASSWORD [50](#)  
INFA\_DEFAULT\_DOMAIN\_USER [51](#)  
INFA\_DEFAULT\_PWX\_OSEPASSWORD [52](#)  
INFA\_DEFAULT\_PWX\_OSPASSWORD [53](#)  
INFA\_JAVA\_CMD\_OPTS [55](#)  
INFA\_NODE\_KEYSTORE\_PASSWORD [57](#)  
INFA\_NODE\_TRUSTSTORE\_PASSWORD [58](#)  
INFA\_PASSWORD [55](#)  
INFA\_REPCNX\_INFO [58](#)  
INFA\_REPOSITORY\_PASSWORD [59](#)  
INFATool\_DATEFORMAT [60](#)  
Konfigurieren von Befehlszeilenprogrammen [44](#)  
UnassignDefaultOSProfile (infacmd isp) [751](#)  
UnassignSMMSservice (infacmd)  
Beschreibung [752](#)  
UnassignLicense (infacmd)  
Beschreibung [754](#)  
UnassignRoleFromGroup (infacmd isp)  
Beschreibung [756](#)  
UnassignRoleFromUser (infacmd isp)  
Beschreibung [758](#)  
UnassignRSWSHubService (infacmd isp)  
Beschreibung [760](#)  
UnassociateDomainNode (infacmd isp)  
Beschreibung [762](#)  
UndeployApplication (infacmd dis) [259](#)  
UndoCheckout (pmrep)  
Beschreibung [1522](#)  
UninstallAbapProgram (pmrep)  
Beschreibung [1533](#)  
unlockObject (infacmd mrs) [952](#)  
Unregister (pmrep)  
Beschreibung [1523](#)  
UnregisterPlugin (pmrep)  
Beschreibung [1524](#)  
UnscheduleWorkflow (pmcmd)  
Beschreibung [1433](#)  
UnsetFolder (pmcmd)  
Beschreibung [1435](#)  
untag  
infacmd dis [254](#)  
updateADLSCertificate (infacmd ccps) [99](#)  
UpdateApplication (infacmd dis) [261](#)  
UpdateApplicationOptions (infacmd dis) [263](#)  
UpdateColumnOptions (infacmd sql) [1203](#)

updateConfiguration (infacmd cluster) [129](#)  
UpdateConnection (infacmd isp)  
description [764](#)  
UpdateConnection (pmrep)  
Beschreibung [1526](#)  
updateCustomLDAPType (infacmd isp)  
Beschreibung [768](#)  
UpdateDataObjectsOptions (infacmd dis) [266](#)  
updateDomainName (infasetup)  
Beschreibung [1367](#)  
UpdateDomainOptions (infacmd isp)  
Beschreibung [771](#)  
updateDomainSamlConfig (infasetup)  
Beschreibung [1376](#)  
UpdateEmailAddr (pmrep)  
Beschreibung [1528](#)  
updateExportXML  
infacmd xrf [1308](#)  
UpdateFolder (infacmd isp)  
Beschreibung [773](#)  
UpdateGatewayInfo (infacmd isp)  
Beschreibung [775](#)  
UpdateGatewayNode (infasetup)  
Beschreibung [1367](#)  
UpdateGrid (infacmd isp)  
Beschreibung [776](#)  
UpdateIntegrationService (infacmd isp)  
Beschreibung [778](#)  
UpdateKerberosAdminUser (infasetup)  
beschreibung [1373](#)  
UpdateKerberosConfig (infasetup)  
Beschreibung [1373](#)  
updateLDAPConnectivity (infacmd isp)  
Beschreibung [781](#)  
UpdateLicense (infacmd isp)  
Beschreibung [784](#)  
UpdateListenerService (infacmd pwx) [1092](#)  
UpdateLoggerService (infacmd pwx) [1096](#)  
updateMappingOptions (infacmd ms) [996](#)  
updateMitKerberosLinkage (infasetup)  
Beschreibung [1374](#)  
UpdateMMService (infacmd isp)  
Beschreibung [786](#)  
UpdateMonitoringOptions (infacmd isp) [788](#)  
UpdateNamespace (infacmd isp) [791](#)  
UpdateNodeOptions (infacmd isp)  
Beschreibung [794](#)  
UpdateNodeRole (infacmd isp) [796](#)  
UpdateOperationOptions  
infacmd ws [1300](#)  
updateOptimizationDefaultLevel (infacmd ms) [998](#)  
updateOptimizationLevel (infacmd ms) [1000](#)  
UpdateOSProfile (infacmd isp)  
Beschreibung [799](#)  
UpdateParameterSetEntries (infacmd dis) [269](#)  
UpdatePasswordComplexityConfig (infasetup) [1376](#)  
UpdateRepositoryService (infacmd isp)  
Beschreibung [802](#)  
updateSamlConfig (infasetup)  
Beschreibung [1376](#)  
UpdateSAPBWService (infacmd isp)  
Beschreibung [807](#)  
UpdateSchedule (infacmd sch) [1146](#)  
UpdateSeqGenVals (pmrep)  
Beschreibung [1529](#)  
updateService (infacmd edp) [322](#)  
updateService (infacmd idp) [309](#)

- UpdateServiceLevel (infacmd isp)
  - Beschreibung [809](#)
- UpdateServiceOptions (infacmd as) [74](#)
- UpdateServiceOptions (infacmd cms) [149](#)
- UpdateServiceOptions (infacmd dis) [271](#)
- UpdateServiceOptions (infacmd mas) [857](#)
- UpdateServiceOptions (infacmd mrs) [954](#)
- UpdateServiceOptions (infacmd rms) [1119](#)
- UpdateServiceOptions (infacmd sch) [1149](#)
- UpdateServiceOptions (infacmd search) [1164](#)
- UpdateServiceProcess (infacmd isp)
  - Beschreibung [810](#)
- UpdateServiceProcessOptions (infacmd as) [75](#)
- UpdateServiceProcessOptions (infacmd cms) [152](#)
- UpdateServiceProcessOptions (infacmd dis) [285](#)
- UpdateServiceProcessOptions (infacmd mas) [860](#)
- UpdateServiceProcessOptions (infacmd mrs) [961](#)
- UpdateServiceProcessOptions (infacmd sch) [1152](#)
- UpdateServiceProcessOptions (infacmd search) [1166](#)
- UpdateSMTPOptions (infacmd isp)
  - Beschreibung [813](#)
- UpdateSQLDataServiceOptions (infacmd sql) [1206](#)
- UpdateSrcPrefix (pmrep)
  - Aktualisieren von nicht wiederverwendbaren Sitzungen [1530](#)
  - Beschreibung [1530](#)
- updateStatistics (infacmd mrs) [963](#)
- UpdateStatistics (pmrep)
  - Beschreibung [1531](#)
- UpdateTableOptions (infacmd sql) [1209](#)
- UpdateTargPrefix (pmrep)
  - Aktualisieren von nicht wiederverwendbaren Sitzungen [1532](#)
  - Beschreibung [1532](#)
- UpdateWebServiceOptions
  - infacmd ws [1303](#)
- UpdateWorkerNode (infasetup)
  - Beschreibung [1379](#)
- UpdateWSHubService (infacmd isp)
  - Beschreibung [815](#)
- Upgrade (infacmd cms) [154](#)
- Upgrade (infacmd sch) [1156](#)
- UpgradeContents (infacmd mrs) [965](#)
- upgradeDomainMetadata
  - Beschreibung [1384](#)
- UpgradeGatewayNodeMetadata (infasetup)
  - Beschreibung [817](#), [1386](#)
- UpgradeModels (infacmd pwx) [1089](#)
- upgradeRepository (infacmd bg) [87](#)
- upgradeService (infacmd edp) [326](#)

## V

- Validate (pmrep)
  - Beschreibung [1535](#)
- ValidateandRegisterFeature (infasetup)
  - beschreibung [1389](#)
- validateFeature (infacmd advanced) [819](#)
- Validieren von Objekten
  - Mit pmrep [1535](#)
- Verbindung
  - Web Content-Kapow Katalyst [495](#)
- Verbindung des parallelen Teradata-Transporters
  - infacmd [490](#)
- Verbindungen
  - Auflisten mit infacmd isp [619](#)
  - Auflisten von Optionen mit infacmd isp [611](#), [621](#)
  - Entfernen aus Domänen mit infacmd isp [689](#)
  - Erstellen mit infacmd [418](#)

- Verbindungen (Fortsetzung)
  - Exportieren mit infacmd isp [560](#)
  - Importieren mit infacmd isp [595](#)
  - Oracle [480](#)
  - Umbenennen mit infacmd [731](#)
- Verbindungsberechtigungen
  - Auflisten für Benutzer oder Gruppen [613](#)
  - Auflisten mit infacmd isp [615](#)
  - Hinzufügen zu Benutzern oder Gruppen [369](#)
- Verbindungsoptionen
  - DB2 für infacmd [456](#)
  - SEQ für infacmd [486](#)
  - VSAM für infacmd [494](#)
- Verbindungsstring
  - Beispiele [1443](#)
  - Syntax [1443](#)
- Vergleichsoperatoren
  - Ordnerpfad [292](#)
  - query [291](#)
- Version (infacmd)
  - Beschreibung [820](#)
- Version (pmcmd)
  - Beschreibung [1435](#)
- Version (pmrep)
  - Beschreibung [1537](#)
- Virtuelle Schemata
  - Auflisten von Berechtigungen [1168](#)
- virtuelle Spalten
  - Auflisten von Berechtigungen [1171](#)
- Virtuelle Spalten
  - Aktualisieren der Optionen [1203](#)
- Virtuelle Tabellen
  - Auflisten von Berechtigungen [1182](#)
  - Auflisten von Eigenschaften für [1180](#)
  - Einrichten von Berechtigungen [1197](#)
  - Konfigurieren von Eigenschaften für [1209](#)
  - Optionen für infacmd [1211](#)
- VSAM
  - infacmd-Verbindungsoptionen [494](#)

## W

- Wait-Modus
  - Konfigurieren mithilfe von pmcmd [1395](#)
- WaitTask (pmcmd)
  - Beschreibung [1435](#)
- WaitWorkflow (pmcmd)
  - Beschreibung [1437](#)
- Web Content-Kapow Katalyst
  - Verbindung [495](#)
- Web-Dienst-Optionen
  - infacmd-Syntax [1305](#)
- Webdienst
  - Aktualisieren von Eigenschaften für [1303](#)
  - Auflisten mit infacmd [1287](#)
  - Auflisten von Berechtigungen [1285](#)
  - Auflisten von Eigenschaften für [1283](#)
  - Beenden mit infacmd [1299](#)
  - Festlegen von Berechtigungen mit infacmd [1294](#)
  - Starten mit infacmd [1297](#)
  - Umbenennen mit infacmd [1289](#)
- Webdienst-Hub
  - Aktualisieren mit infacmd isp [815](#)
  - Erstellen in einer Domäne [536](#)
  - Trennen eines Repository mit infacmd isp [760](#)
  - Verbinden eines Repository mit infacmd isp [412](#)

## Webdienstvorgang

- Aktualisieren von Eigenschaften für [1300](#)

- Auflisten von Berechtigungen [1281](#)

- Auflisten von Eigenschaften für [1279](#)

- Festlegen von Berechtigungen mit infacmd [1291](#)

## Where-Klausel

- query [295](#)

## Wiederherstellen

- Repositories mit pmrep Restore [1517](#)

## X

### XML-Datei

- Plug-In-Vorlagen [1516](#)

## Z

### Zeitzone

- gültige Werte für Zeitplan [1133](#)

### Zuordnungen

- Auflisten [981](#), [987](#)

### Zuordnungsausgaben

- Aktualisieren mit infacmd [1269](#)

### Zuordnungsoptionen

- Aktualisieren [996](#)

### Zuordnungsprotokoll

- Zugreifen mit infacmd ms [979](#)

Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen. (infacmd cms) [143](#)