



Informatica®

10.5

Référence des commandes

© Copyright Informatica LLC 1998, 2021

Ce logiciel et la documentation associée sont fournis uniquement sous un accord de licence séparé contenant des restrictions d'utilisation et de divulgation. Il est interdit de reproduire ou de transmettre sous quelle que forme et par quel que moyen que ce soit (électronique, photocopie, enregistrement ou autre) tout ou partie de ce document sans le consentement préalable d'Informatica LLC.

Informatica, le logo Informatica, PowerCenter, PowerExchange, Big Data Management et Enterprise Data Catalog sont des marques ou des marques déposées d'Informatica LLC aux États-Unis et dans de nombreux autres pays. Une liste actuelle des marques déposées d'Informatica est disponible sur le site <https://www.informatica.com/trademarks.html>. Les autres noms de société ou de produit peuvent être des marques de commerce ou des marques déposées de leurs détenteurs respectifs.

U.S. GOVERNMENT RIGHTS Les programmes, les logiciels, les bases de données et les documents connexes et les données techniques fournis aux clients du gouvernement américain sont des « logiciels commerciaux » ou des « données techniques commerciales », conformément au règlement fédéral sur les acquisitions et aux règlements supplémentaires propres à l'Agence. En tant que tel, l'utilisation, la duplication, la divulgation, la modification et l'adaptation sont assujetties aux restrictions et aux conditions de licence énoncées dans le contrat gouvernemental applicable et, dans la mesure applicable par les termes du contrat gouvernemental, les droits additionnels énoncés dans la réglementation FAR 52.227-19, licence de logiciel d'ordinateur commercial.

Certaines parties de ce logiciel et/ou de cette documentation sont soumises à des droits d'auteur détenus par des tiers. Les notifications de tiers requises sont incluses avec le produit.

Les renseignements contenus dans cette documentation sont sujets à modification sans préavis. Si vous constatez des problèmes liés à la documentation, merci de les signaler par courriel à l'adresse infa_documentation@Informatica.com.

Les produits Informatica sont garantis conformément aux termes et conditions des accords en vertu desquels ils sont fournis. INFORMATICA FOURNIT LES INFORMATIONS DE CE DOCUMENT « EN L'ÉTAT » SANS GARANTIE D'AUCUNE SORTE, EXPRESSE OU IMPLICITE, NOTAMMENT AUCUNE GARANTIE DE QUALITÉ MARCHANDE, D'ADAPTATION À UN USAGE PARTICULIER ET D'ABSENCE DE CONTREFAÇON

Date de publication: 2021-05-10

Sommaire

Préface.....	27
Ressources Informatica.	27
Informatica Network.	27
Base de connaissances Informatica.	27
Documentation Informatica.	28
Matrices de disponibilité des produits Informatica.	28
Informatica Velocity.	28
Informatica Marketplace.	28
Support client international Informatica.	28
 Chapitre 1: Programmes et utilitaires de ligne de commande.....	 29
Présentation des programmes et utilitaires de ligne de commande.	29
 Chapitre 2: Installation et configuration des utilitaires de ligne de commande.....	 31
Installation et configuration des utilitaires de ligne de commande - Présentation.	31
Installation des utilitaires de ligne de commande.	32
Répertoires d'installation.	32
Configuration des utilitaires de ligne de commande.	33
Configurer les utilitaires Informatica.	33
Configurer les utilitaires PowerCenter.	33
Configurer les utilitaires Metadata Manager.	34
Créer le fichier domains.infa.	34
Configuration de sécurité pour les utilitaires Informatica	35
 Chapitre 3: Utilisation des programmes de ligne de commande.....	 36
Présentation de l'utilisation des programmes de ligne de commande.	36
Entrée d'options et d'arguments.	37
Notation de syntaxe.	38
Exécution de commandes dans un domaine sécurisé.	39
Exécution de commandes sous UNIX avec l'authentification Kerberos.	40
Exécution de commandes sous UNIX avec l'authentification unique.	40
Exécution de commandes sous UNIX sans l'authentification unique.	41
Exécution de commandes sous Windows avec l'authentification Kerberos.	42
 Chapitre 4: Variables d'environnement pour les programmes de ligne de commande.....	 43
Présentation des variables d'environnement pour les programmes de ligne de commande.	44
ICMD_JAVA_OPTS.	46
Configuration d'ICMD_JAVA_OPTS sous UNIX.	46

Configuration d'ICMD_JAVA_OPTS sous Windows.	46
INFA_CLIENT_RESILIENCE_TIMEOUT.	46
Configuration d'INFA_CLIENT_RESILIENCE_TIMEOUT sous UNIX.	47
Configuration d'INFA_CLIENT_RESILIENCE_TIMEOUT sous Windows.	47
INFA_CODEPAGENAME.	47
Configuration d'INFA_CODEPAGENAME sous UNIX.	47
Configuration d'INFA_CODEPAGENAME sous Windows.	48
INFA_DEFAULT_DATABASE_PASSWORD.	48
Configuration d'INFA_DEFAULT_DATABASE_PASSWORD sous UNIX.	48
Configuration d'INFA_DEFAULT_DATABASE_PASSWORD sous Windows.	49
INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD.	49
Configuration de INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD sous UNIX.	49
Configuration de INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD sous Windows.	50
INFA_DEFAULT_DOMAIN.	50
Configuration d'INFA_DEFAULT_DOMAIN sous UNIX.	50
Configuration d'INFA_DEFAULT_DOMAIN sous Windows.	50
INFA_DEFAULT_DOMAIN_PASSWORD.	50
Configuration d'INFA_DEFAULT_DOMAIN_PASSWORD sous UNIX.	51
Configuration d'INFA_DEFAULT_DOMAIN_PASSWORD sous Windows.	51
INFA_DEFAULT_DOMAIN_USER.	51
Configuration d'INFA_DEFAULT_DOMAIN_USER sous UNIX.	52
Configuration d'INFA_DEFAULT_DOMAIN_USER sous Windows.	52
INFA_DEFAULT_PWX_OSEPASSWORD.	52
Configuration d'INFA_DEFAULT_PWX_OSEPASSWORD sous UNIX.	52
Configuration d'INFA_DEFAULT_PWX_OSEPASSWORD sous Windows.	53
INFA_DEFAULT_PWX_OSPASSWORD.	53
Configuration d'INFA_DEFAULT_PWX_OSPASSWORD sous UNIX.	53
Configuration d'INFA_DEFAULT_PWX_OSPASSWORD sous Windows.	53
INFA_DEFAULT_SECURITY_DOMAIN.	53
Configuration d'INFA_DEFAULT_SECURITY_DOMAIN sous UNIX.	54
Configuration d'INFA_DEFAULT_SECURITY_DOMAIN sous Windows.	54
INFA_DOMAINS_FILE.	54
Configuration d'INFA_DOMAINS_FILE sous UNIX.	54
Configuration d'INFA_DOMAINS_FILE sous Windows.	55
INFA_JAVA_CMD_OPTS.	55
Configuration d'INFA_JAVA_CMD_OPTS sous UNIX.	55
Configuration d'INFA_JAVA_CMD_OPTS sous Windows.	55
INFA_PASSWORD.	55
Configuration d'INFA_PASSWORD sous UNIX.	56
Configuration d'INFA_PASSWORD sous Windows.	56
INFA_NODE_KEYSTORE_PASSWORD.	57
Configuration de INFA_NODE_KEYSTORE_PASSWORD sous UNIX.	57

Configuration de INFA_NODE_KEYSTORE_PASSWORD sous Windows.	57
INFA_NODE_TRUSTSTORE_PASSWORD.	58
Configuration de INFA_NODE_TRUSTSTORE_PASSWORD sous UNIX.	58
Configuration de INFA_NODE_TRUSTSTORE_PASSWORD sous Windows.	58
INFA_REPCNX_INFO.	58
Configuration d'INFA_REPCNX_INFO sous UNIX.	59
Configuration d'INFA_REPCNX_INFO sous Windows.	59
INFA_REPOSITORY_PASSWORD.	59
Configuration d'INFA_REPOSITORY_PASSWORD sous UNIX.	60
Configuration d'INFA_REPOSITORY_PASSWORD sous Windows.	60
INFATool_DATEFORMAT.	60
Configuration d'INFATool_DATEFORMAT sous UNIX.	60
Configuration d'INFATool_DATEFORMAT sous Windows.	61
Chiffrement des mots de passe.	61
Utilisation d'un Mot de Passe en tant que variable d'environnement.	62
Définition du nom d'utilisateur.	63
Configuration d'un Nom d'Utilisateur en tant que variable d'environnement sous UNIX.	63
Configuration d'un Nom d'Utilisateur en tant que variable d'environnement sous Windows.	63
Chapitre 5: Utilisation d'infacmd.	64
Utilisation d'infacmd, présentation.	64
infacmd ListPlugins.	65
Exécution de commandes.	65
Connexion au domaine.	66
Codes de retour infacmd.	67
Chapitre 6: infacmd comme Référence de commande.	68
CreateExceptionAuditTables.	68
CreateService.	70
DeleteExceptionAuditTables.	72
ListServiceOptions.	73
ListServiceProcessOptions.	73
UpdateServiceOptions.	74
UpdateServiceProcessOptions.	75
Chapitre 7: infacmd and Command Reference.	77
getDomainObjectPermissions.	77
getPrivilegeAssociation.	78
getUserGroupAssociation.	80
getUserGroupAssociationForRoles.	81
getUsersPersonalInfo.	82

Chapitre 8: Référence de commande infacmd autotune.....	85
Autotune.	85
Chapitre 9: Référence de commande infacmd bg.....	87
upgradeRepository.	87
deleteAuditHisotry.	88
listGlossary.	89
exportGlossary.	90
importGlossary.	92
Chapitre 10: Référence de commande infacmd ccps.....	95
deleteClusters.	95
listClusters.	97
updateADLSCertificate.	99
Chapitre 11: Référence de commande de cluster infacmd	101
createConfiguration.	101
createConfigurationWithParams.	104
deleteConfiguration.	106
clearConfigurationProperties.	108
exportConfiguration.	110
listAssociatedConnections.	112
listConfigurationGroupPermissions.	113
listConfigurationSets.	115
listConfigurationProperties.	116
listConfigurations.	118
listConfigurationUserPermissions.	120
refreshConfiguration.	121
setConfigurationPermissions.	123
setConfigurationProperties.	125
updateConfiguration.	127
Chapitre 12: Référence de commande infacmd CMS.....	130
CreateAuditTables.	130
CreateService.	132
DeleteAuditTables.	134
ListServiceOptions.	136
ListServiceProcessOptions.	138
Purge.	139
RemoveService.	141
ResyncData.	143
UpdateServiceOptions.	145

UpdateServiceProcessOptions.	148
Mise à niveau.	150
Chapitre 13: référence de commande infacmd dis.....	152
AddParameterSetEntries.	153
BackupApplication.	155
CancelDataObjectCacheRefresh.	157
CreateService.	159
compareMapping.	162
compareObject.	166
DeleteParameterSetEntries.	170
deployObjectsToFile.	172
DeployApplication.	176
disableMappingValidationEnvironment.	178
enableMappingValidationEnvironment.	180
ListApplicationObjectPermissions.	183
ListApplicationObjects.	185
ListApplicationOptions.	187
ListApplicationPermissions.	189
ListApplications.	190
ListComputeOptions.	192
ListDataObjectOptions.	193
ListMappingEngines.	195
ListParameterSetEntries.	198
ListParameterSetObjects.	200
ListParameterSets.	201
listPatchNames.	203
ListSequenceObjectProperties.	204
ListSequenceObjects.	206
ListServiceOptions.	208
ListServiceProcessOptions.	210
PurgeDataObjectCache.	211
PurgeResultSetCache.	213
queryDesignTimeObjects.	215
queryRunTimeObjects.	217
RefreshDataObjectCache.	218
RenameApplication.	220
replaceMappingHadoopRuntimeConnections.	222
RestoreApplication.	224
SetApplicationPermissions.	226
SetApplicationObjectPermissions.	228
setMappingExecutionEnvironment.	230
SetSequenceState.	232

StartApplication.	235
StopApplication.	236
stopBlazeService.	238
tag.	241
untag.	243
replaceAllTag.	246
UndeployApplication.	249
UpdateApplication.	250
UpdateApplicationOptions.	252
UpdateComputeOptions.	254
UpdateDataObjectOptions.	256
Options des objets de données.	258
UpdateParameterSetEntries.	259
UpdateServiceOptions	261
Options du service d'intégration de données.	263
UpdateServiceProcessOptions	275
Options du processus de service d'intégration de données.	277
Règles et directives.	278
 Chapitre 14: Requêtes infacmd dis.....	 280
Requêtes.	280
Opérateurs de comparaison.	281
Spécification d'un chemin de dossier.	282
Opérateurs logiques.	283
Paramètres de requête.	283
Structure de requête.	285
Clause Where.	286
 Chapitre 15: Référence de commande infacmd dp.....	 287
startSparkJobServer.	287
stopSparkJobServer.	289
 Chapitre 16: Référence de commande infacmd idp.....	 291
createRepository.	291
createService.	293
updateService.	297
upgradeRepository.	300
 Chapitre 17: Référence de commande infacmd edp.....	 303
createService.	303
purgeauditevents.	307
updateService.	310
upgradeService.	313

Chapitre 18: Référence de commande infacmd es.....	316
ListServiceOptions.	316
UpdateServiceOptions.	317
UpdateSMTPOptions.	318
 Chapitre 19: Référence de commande infacmd ics.....	 321
cleanCluster.	321
createservice.	323
ListServiceOptions.	334
ListServiceProcessOptions.	335
shutdownCluster.	337
UpdateServiceOptions.	338
UpdateServiceProcessOptions.	340
 Chapitre 20: Référence de commande infacmd ipc.....	 342
ExportToPC.	342
ImportFromPC.	346
genReuseReportFromPC.	348
 Chapitre 21: Référence de commande infacmd isp.....	 352
AddAlertUser.	352
AddConnectionPermissions.	354
addCustomLDAPType.	356
AddDomainLink.	359
AddDomainNode.	361
AddGroupPrivilege.	363
addLDAPConnectivity	365
AddLicense.	368
AddNamespace.	370
AddNodeResource.	373
AddRolePrivilege.	375
AddServiceLevel.	377
AddUserPrivilege.	379
AddUserToGroup	381
AssignDefaultOSProfile.	383
AssignedToLicense.	385
AssignGroupPermission	386
AssignISToMMSservice.	388
AssignLicense.	390
AssignRoleToGroup.	392
AssignRoleToUser	394
AssignRSToWSHubService.	396

AssignUserPermission	398
ConvertLogFile.	400
convertUserActivityLogFile.	401
CreateConnection.	402
Options de connexion ADABAS.	407
Options de connexion Amazon Kinesis	409
Options de connexion d'Amazon Redshift.	410
Options de connexion Amazon S3.	412
Options de connexion de blockchain.	414
Options de connexion Cassandra.	416
Options de connexion Confluent Kafka.	417
Options de connexion Databricks.	417
Options de connexion DataSift.	418
Options de connexion DB2 pour i5/OS.	419
Options de connexion DB2 for z/OS.	421
Options de connexion Facebook.	423
Options de connexion Greenplum.	424
Options de connexion Google Analytics.	425
Options de connexion Google BigQuery.	425
Options de connexion Google Cloud Spanner.	426
Options de connexion Google Cloud Storage.	427
Options de connexion Hadoop.	428
Options de connexion HBase.	433
Options de connexion HDFS.	434
Options de connexion Hive.	434
Options de connexion IBM DB2.	438
Options de connexion IMS.	441
Options de connexion JDBC.	443
Options de connexion JDBC V2.	445
Options de connexion JD Edwards EnterpriseOne.	447
Options de connexion Kafka.	448
Options de connexion Kudu.	449
Options de connexion LDAP.	449
Options de connexion LinkedIn.	450
Options de connexion MapR-DB.	451
Options de connexion de stockage Blob Microsoft Azure.	451
Options de connexion Microsoft Azure Data Lake Storage Gen1.	452
Options de connexion Microsoft Azure Data Lake Storage Gen2.	452
Options de connexion Microsoft Azure SQL Data Warehouse.	453
Options de connexion Microsoft SQL Server.	454
Options de connexion Microsoft Dynamics CRM.	457
Options de connexion Netezza.	459

Options de connexion OData.	460
Options de connexion ODBC.	460
Options de connexion Oracle.	462
Options de connexion Salesforce.	465
Options de connexion Salesforce Marketing Cloud.	466
Options de connexion SAPAPPLICATIONS.	468
Options de connexion séquentielle.	468
Options de connexion Snowflake.	470
Options de connexion Tableau.	471
Options de connexion Tableau V3.	472
Options de connexion Teradata Parallel Transporter.	473
Options de connexion Twitter.	475
Options de connexion Twitter Streaming.	476
Options de connexion VSAM.	476
Options de connexion Web Content-Kapow Katalyst.	478
CreateFolder.	479
CreateGrid.	480
CreateGroup.	482
CreateIntegrationService.	484
Options du service d'intégration.	488
Options du processus de service d'intégration.	492
CreateMMSservice.	494
Options du service Metadata Manager	496
CreateOSProfile	498
Options des processus de service d'intégration de données pour les profils de système d'exploitation.	501
Options des processus de service d'intégration PowerCenter pour les profils de système d'exploitation.	502
CreateRepositoryService.	504
CreateRole.	509
CreateSAPBWService.	510
Options du service SAP BW.	513
Option de processus de service SAP BW.	514
CreateUser	514
CreateWSHubService.	517
Options du Hub de services Web.	520
DeleteNamespace.	521
DisableNodeResource.	523
DisableService.	525
DisableServiceProcess.	527
DisableUser.	529
EditUser.	531
EnableNodeResource.	534

EnableService.	535
EnableServiceProcess.	537
EnableUser	539
ExportDomainObjects.	541
ExportUsersAndGroups.	544
GetFolderInfo.	546
GetLastError.	548
GetLog.	550
GetNodeName.	553
GetPasswordComplexityConfig.	554
getDomainSamlConfig.	555
GetServiceOption.	557
GetServiceProcessOption.	558
GetServiceProcessStatus.	560
GetServiceStatus.	562
GetSessionLog.	563
GetSystemLogDirectory.	567
getUserActivityLog.	567
GetWorkflowLog.	570
Aide.	573
ImportDomainObjects.	574
ImportUsersAndGroups.	579
ListAlertUsers.	581
listAllCustomLDAPTypes.	583
ListAllGroups.	584
listAllLDAPConnectivity.	586
ListAllRoles	587
ListAllUsers	589
ListConnectionOptions.	590
ListConnectionPermissions.	592
ListConnectionPermissionsByGroup.	594
ListConnectionPermissionsByUser.	596
ListConnections.	598
ListConnectionOptions.	600
listCustomLDAPType.	601
ListDefaultOSProfiles.	603
ListDomainCiphers.	604
ListDomainLinks.	607
ListDomainOptions.	608
ListFolders.	610
ListGridNodes.	611
ListGroupPermissions.	613

ListGroupPrivileges.	615
ListGroupsForUser.	616
ListLDAPConnectivity.	618
ListLicenses.	620
ListMonitoringOptions.	622
ListNodeOptions.	623
ListNodeResources.	625
ListNodeRoles.	626
ListNodes.	628
ListOSProfiles.	630
ListRepositoryLDAPConfiguration.	632
ListRolePrivileges.	633
ListSecurityDomains.	635
ListServiceLevels.	636
ListServiceNodes.	638
ListServicePrivileges.	639
ListServices.	641
ListSMTPOptions.	643
ListUserPermissions.	645
ListUserPrivileges.	647
infacmd ListWeakPasswordUsers.	649
migrateUsers.	650
MoveFolder.	652
MoveObject.	654
Ping.	656
PingDomain.	657
PrintSPNAndKeytabNames.	659
PurgeLog.	660
PurgeMonitoringData.	662
RemoveAlertUser.	664
RemoveConnection.	666
RemoveConnectionPermissions.	668
removeCustomLDAPType.	670
RemoveDomainLink.	672
RemoveFolder.	674
RemoveGrid.	675
RemoveGroup.	677
RemoveGroupPermission.	678
RemoveGroupPrivilege.	680
removeLDAPConnectivity.	682
RemoveLicense.	684
RemoveNode.	686

RemoveNodeResource.	687
RemoveOSProfile.	689
RemoveRole	691
RemoveRolePrivilege	692
RemoveService.	694
RemoveServiceLevel.	696
RemoveUser.	697
RemoveUserFromGroup	699
RemoveUserPermission	700
RemoveUserPrivilege	703
RenameConnection.	705
ResetPassword.	707
RunCPUProfile.	709
SetConnectionPermissions.	711
SetRepositoryLDAPConfiguration	713
ShowLicense.	716
ShutdownNode.	717
SwitchToGatewayNode.	719
SwitchToWorkerNode.	721
SyncSecurityDomains.	723
UnassignDefaultOSProfile.	725
UnassignISMMSservice.	726
UnassignLicense.	728
UnassignRoleFromGroup	730
UnassignRoleFromUser.	731
UnassignRSWSHubService.	734
UnassociateDomainNode.	735
UpdateConnection.	737
updateCustomLDAPType.	741
UpdateDomainOptions.	744
UpdateFolder.	746
UpdateGatewayInfo	748
UpdateGrid.	749
UpdateIntegrationService.	751
updateLDAPConnectivity.	753
UpdateLicense.	756
UpdateMMSservice.	758
UpdateMonitoringOptions.	760
UpdateNamespace.	763
UpdateNodeOptions.	766
UpdateNodeRole.	768
UpdateOSProfile.	771

UpdateRepositoryService.	774
UpdateSAPBWService.	779
UpdateServiceLevel.	781
UpdateServiceProcess.	782
UpdateSMTPOptions.	784
UpdateWSHubService.	786
UpgradeGatewayNodeMetadata.	788
validateFeature.	790
Version.	792

Chapitre 22: Référence de commande infacmd ldm..... 793

BackupContents.	793
CreateService.	796
ListServiceOptions.	802
ListServiceProcessOptions.	803
migrateContents.	805
publishArchive.	807
restoreContents.	809
UpdateServiceOptions.	811
UpdateServiceProcessOptions.	813
mise à niveau.	815

Chapitre 23: Référence de commande infacmd mas..... 817

CreateService.	817
ListServiceOptions.	821
ListServiceProcessOptions.	823
UpdateServiceOptions.	825
Options du service d'accès aux métadonnées.	827
UpdateServiceProcessOptions.	828
Options de processus de service d'accès aux métadonnées.	830

Chapitre 24: Référence de commande infacmd mi..... 831

abortRun.	831
clearSamlConfig.	832
createService.	833
deploySpec.	836
exportSpec.	838
extendedRunStats.	839
getSpecRunStats.	841
listSpecRuns.	842
listSpecs.	843
restartMapping.	844
runSpec.	845

updateSamlConfig.	847
---------------------------	-----

Chapitre 25: Référence de commande infacmd mrs..... 850

BackupContents.	851
CheckInObject.	853
CreateContents.	855
CreateFolder.	857
CreateProject.	858
CreateService.	860
DeleteContents.	864
DeleteFolder.	866
DeleteProject.	868
disableMappingValidationEnvironment.	870
enableMappingValidationEnvironment.	872
ListBackupFiles.	875
ListCheckedOutObjects.	876
listFolders.	878
ListLockedObjects.	880
listMappingEngines.	882
listPermissionOnProject.	884
ListProjects.	886
ListServiceOptions.	888
ListServiceProcessOptions.	889
ManageGroupPermissionOnProject.	891
ManageUserPermissionOnProject.	893
PopulateVCS.	895
ReassignCheckedOutObject.	896
rebuildDependencyGraph.	898
RenameFolder.	900
replaceMappingHadoopRuntimeConnections.	901
RestoreContents.	903
UndoCheckout.	905
setMappingExecutionEnvironment.	907
UndoCheckout.	909
UnlockObject.	911
UpdateServiceOptions.	913
Options du service de référentiel modèle.	915
UpdateServiceProcessOptions.	920
UpdateStatistics.	921
UpgradeContents.	923
UpgradeExportedObjects.	925

Chapitre 26: Référence de commande d'infacmd ms	927
abortAllJobs.	927
deleteMappingPersistedOutputs.	929
fetchAggregatedClusterLogs.	931
getMappingStatus.	933
getRequestLog.	935
ListMappingOptions.	937
listMappingParams.	939
Sortie de listMappingParams.	941
listMappingPersistedOutputs.	941
listMappings.	943
purgeDatabaseWorkTables.	945
runMapping.	947
UpdateMappingOptions.	952
UpdateOptimizationDefaultLevel.	954
UpdateOptimizationLevel.	956
upgradeMappingParameterFile.	958
 Chapitre 27: Référence de commande infacmd oie.....	 961
 Chapitre 28: Référence de commande infacmd ps.....	 962
cancelProfileExecution.	962
CreateWH.	964
detectOrphanResults.	966
DropWH.	967
Exécuter.	969
executeProfile.	971
getExecutionStatus.	973
getProfileExecutionStatus.	975
Liste.	977
ListAllProfiles.	979
migrateProfileResults.	980
migrateScorecards.	982
Purger.	984
purgeOrphanResults.	986
restoreProfilesAndScorecards.	988
synchronizeProfile.	990
 Chapitre 29: Référence de commande infacmd pwx.....	 992
CloseForceListener.	993
CloseListener.	995
CondenseLogger.	998

createdatamaps.	1000
CreateListenerService.	1003
CreateLoggerService.	1006
DisplayAllLogger.	1010
DisplayCPULogger.	1013
DisplayEventsLogger.	1015
DisplayMemoryLogger.	1018
DisplayRecordsLogger.	1020
displayStatsListener.	1024
DisplayStatusLogger.	1027
FileSwitchLogger.	1030
ListTaskListener.	1032
ShutDownLogger.	1035
StopTaskListener.	1038
UpgradeModels.	1041
UpdateListenerService.	1043
UpdateLoggerService.	1046
 Chapitre 30: Référence de commande infacmd roh.	 1052
listProcessProperties.	1052
listReverseProxyServerOptions.	1054
listServiceProcessOptions.	1055
listServiceOptions.	1057
updateReverseProxyServerOptions.	1058
updateServiceProcessOptions.	1060
updateServiceOptions.	1062
 Chapitre 31: Référence de commande infacmd rms.	 1064
ListComputeNodeAttributes.	1064
ListServiceOptions.	1066
SetComputeNodeAttributes.	1067
UpdateServiceOptions.	1069
Options du service du gestionnaire de ressource.	1071
 Chapitre 32: Référence de commande infacmd rtm.	 1072
DeployImport.	1072
Exporter.	1074
Import.	1077
 Chapitre 33: Référence de commande infacmd sch.	 1080
CreateSchedule.	1080
Paramètres de fuseau horaire valides.	1083
DeleteSchedule.	1087

ListSchedule.	1088
ListServiceOptions.	1090
ListServiceProcessOptions.	1090
PauseAll.	1092
PauseSchedule.	1092
ResumeAll.	1093
ResumeSchedule.	1094
UpdateSchedule.	1095
UpdateServiceOptions.	1098
Options du service de planificateur.	1100
UpdateServiceProcessOptions.	1101
Options du processus de service de planificateur.	1102
Mise à niveau.	1103
Chapitre 34: Référence de commande infacmd search.	1105
CreateService.	1105
ListServiceOptions.	1108
ListServiceProcessOptions.	1110
UpdateServiceOptions.	1111
UpdateServiceProcessOptions.	1113
Chapitre 35: Référence de commande infacmd sql.	1116
ExecuteSQL.	1117
ListColumnOptions.	1117
ListColumnPermissions.	1119
ListSQLDataServiceOptions.	1121
ListSQLDataServicePermissions.	1123
ListSQLDataServices.	1124
ListStoredProcedurePermissions.	1126
ListTableOptions.	1127
ListTablePermissions.	1129
PurgeTableCache.	1131
RefreshTableCache	1133
RenameSQLDataService.	1134
SetColumnPermissions.	1136
SetSQLDataServicePermissions.	1138
SetStoredProcedurePermissions.	1141
SetTablePermissions.	1143
StartSQLDataService.	1146
StopSQLDataService.	1148
UpdateColumnOptions.	1150
Options de colonne.	1152
UpdateSQLDataServiceOptions.	1152

Options du service de données SQL.	1154
UpdateTableOptions.	1156
Options de la table virtuelle.	1158
Chapitre 36: Référence de commande infacmd tdm.	1159
CreateService.	1159
CreateContents.	1166
EnableService.	1168
DisableService.	1169
Chapitre 37: Référence de commande infacmd tools.	1172
deployApplication.	1172
exportObjects.	1174
exportResources.	1177
importObjects.	1179
patchApplication.	1185
Chapitre 38: Référence de la commande infacmd wfs.	1188
abortWorkflow.	1188
bulkComplete.	1190
cancelWorkflow.	1192
completeTask.	1194
createTables.	1196
delegateTask.	1198
dropTables.	1200
listActiveWorkflowInstances.	1201
listMappingPersistedOutputs.	1203
listTasks.	1205
listWorkflowParams.	1208
Sortie listWorkflowParams.	1210
listWorkflows.	1211
pruneOldInstances.	1212
recoverWorkflow.	1214
releaseTask.	1216
setMappingPersistedOutputs.	1218
startTask.	1221
startWorkflow.	1222
upgradeWorkflowParameterFile.	1224
Chapitre 39: Référence de commande infacmd ws.	1227
ListOperationOptions.	1227
ListOperationPermissions.	1229
ListWebServiceOptions.	1231

ListWebServicePermissions.	1233
ListWebServices.	1235
RenameWebService.	1236
SetOperationPermissions.	1238
SetWebServicePermissions.	1241
StartWebService.	1244
StopWebService.	1246
UpdateOperationOptions.	1247
Options d'opération.	1249
UpdateWebServiceOptions.	1249
Options du service Web.	1251

Chapitre 40: Référence de la commande infacmd xrf..... 1253

generateReadableViewXML.	1253
updateExportXML.	1254

Chapitre 41: Fichiers de contrôle infacmd..... 1255

Présentation des fichiers de contrôle infacmd.	1255
Configuration du fichier de contrôle.	1256
Conventions de nommage du fichier de contrôle.	1256
Fichiers de contrôle d'exportation.	1257
Paramètres du fichier de contrôle d'exportation pour les objets de domaine.	1257
Paramètres du fichier de contrôle d'exportation pour les objets du référentiel modèle.	1259
Fichiers de contrôle d'importation.	1261
Paramètres du fichier de contrôle d'importation pour les objets de domaine.	1262
Paramètres du fichier de contrôle d'importation pour les objets du référentiel modèle.	1264
Règles et directives concernant les fichiers de contrôle.	1269
Exemples de fichier de contrôle pour les objets de domaine.	1270
Exemples de fichier de contrôle pour les objets du référentiel modèle.	1271

Chapitre 42: Référence de commande infasetup..... 1273

Utilisation d'infasetup.	1274
Exécution de commandes.	1274
Options de commande.	1274
Codes de retour infasetup.	1274
Utilisation des chaînes de connexion à la base de données.	1275
BackupDomain.	1275
DefineDomain.	1278
DefineGatewayNode.	1288
DefineWorkerNode.	1294
DeleteDomain.	1298
GenerateEncryptionKey.	1301
Aide.	1301

ListDomainCiphers.	1302
MigrateEncryptionKey.	1303
RestoreDomain.	1303
restoreMitKerberosLinkage.	1306
SwitchToKerberosMode.	1307
UpdateDomainCiphers.	1308
updateDomainName.	1311
UpdateGatewayNode.	1311
UpdateKerberosAdminUser.	1317
UpdateKerberosConfig.	1317
updateMitKerberosLinkage.	1318
UpdatePasswordComplexityConfig.	1319
UpdateDomainSamlConfig.	1320
UpdateWorkerNode.	1323
upgradeDomainMetadata.	1328
UpgradeGatewayNodeMetadata.	1329
UnlockUser.	1331
ValidateandRegisterFeature.	1332

Chapitre 43: Référence de commande pmcmd. 1334

Utilisation de pmcmd.	1335
Exécution de commandes en mode ligne de commande.	1335
Exécution de commandes en mode interactif.	1337
Exécution en mode attente.	1338
Création de scripts de commandes pmcmd.	1338
Entrée d'options de commande.	1339
aborttask.	1340
abortworkflow.	1342
Connect.	1344
Déconnecter.	1345
Exit.	1345
getrunningsessionsdetails.	1346
GetServiceDetails.	1347
getserviceproperties.	1349
getsessionsstatistics.	1350
gettaskdetails.	1352
getworkflowdetails.	1354
help.	1357
pingservice.	1358
recoverworkflow.	1359
scheduleworkflow.	1361
SetFolder.	1362
SetNoWait.	1363

SetWait.	1363
ShowSettings.	1363
StartTask.	1364
Utilisation des fichiers de paramètres avec StartTask.	1366
StartWorkflow.	1367
Utilisation des fichiers de paramètres avec StartWorkflow.	1369
StopTask.	1370
StopWorkflow.	1372
UnscheduleWorkflow.	1374
UnsetFolder.	1375
Version.	1376
WaitTask.	1376
WaitWorkflow.	1378

Chapitre 44: Référence de commande pmrep..... 1380

Utilisation de pmrep.	1382
Exécution de commandes en mode ligne de commande.	1382
Exécution de commandes en mode interactif.	1382
Exécution de commandes en mode normal et mode exclusif.	1383
Codes de retour pmrep.	1383
Utilisation des chaînes de connexion natives.	1383
Création de scripts de commandes pmrep.	1384
Sous-types de connexion.	1384
AddToDeploymentGroup.	1387
ApplyLabel.	1389
AssignIntegrationService.	1391
AssignPermission.	1392
Exemple.	1393
BackUp.	1393
ChangeOwner.	1394
CheckIn.	1395
CleanUp.	1396
ClearDeploymentGroup.	1396
Connect.	1397
Créer.	1399
CreateConnection.	1400
Spécification de la page de code de la base de données.	1403
CreateDeploymentGroup.	1403
CreateFolder.	1404
Attribution des autorisations.	1405
CreateLabel.	1406
CreateQuery.	1406
Supprimer.	1412

DeleteConnection.	1413
DeleteDeploymentGroup.	1414
DeleteFolder.	1414
DeleteLabel.	1414
DeleteObject.	1415
DeleteQuery.	1416
DeployDeploymentGroup.	1416
DeployFolder.	1418
ExecuteQuery.	1419
Exit.	1421
FindCheckout.	1421
GetConnectionDetails.	1423
GenerateAbapProgramToFile.	1423
Aide.	1425
InstallAbapProgram.	1425
KillUserConnection.	1427
ListConnections.	1428
ListObjectDependencies.	1428
ListObjects.	1431
Liste des types d'objets.	1433
Liste des dossiers.	1435
Liste des objets.	1436
ListTablesBySess.	1436
ListUserConnections.	1437
MassUpdate.	1438
Types de propriété de session.	1440
Règles et instructions pour MassUpdate.	1443
Exemple de fichier journal.	1444
ModifyFolder.	1444
Notification.	1446
ObjectExport.	1446
Exemples.	1448
ObjectImport.	1448
PurgeVersion.	1449
Exemples.	1451
Enregistrement.	1451
RegisterPlugin.	1453
Enregistrement d'un module de sécurité.	1454
Exemple.	1454
Restaurer.	1455
Exemple.	1456
RollbackDeployment.	1456

Exemple.	1457
Exécuter.	1457
ShowConnectionInfo.	1458
SwitchConnection.	1459
TruncateLog.	1459
UndoCheckout.	1460
Désinscrire.	1461
UnregisterPlugin.	1462
Désinscription d'un module de sécurité externe.	1463
Exemple.	1464
UpdateConnection.	1464
UpdateEmailAddr.	1466
UpdateSeqGenVals.	1467
UpdateSrcPrefix.	1468
UpdateStatistics.	1469
UpdateTargPrefix.	1470
Mise à niveau.	1471
UninstallAbapProgram.	1471
Valider.	1473
Version.	1475

Chapitre 45: Utilisation de l'utilitaire filemanager..... 1476

Présentation de filemanager.	1476
copy.	1478
copyfromlocal.	1479
list.	1480
move.	1481
remove.	1482
rename.	1484
watch.	1485

Chapitre 46: Utilisation de pmrep Files..... 1487

Utilisation de pmrep Files Overview.	1487
Utilisation du fichier d'entrée persistant	1487
Création d'un fichier d'entrée persistant avec pmrep.	1488
Création manuelle d'un fichier d'entrée persistant.	1489
Utilisation du fichier de contrôle de l'importation d'objet.	1490
Paramètres du fichier de contrôle de l'importation d'objets.	1491
Exemples du fichier de contrôle de l'importation d'objets.	1494
Importation d'objets source.	1495
Importation de plusieurs objets dans un dossier.	1496
Archivage et libellé d'objets importés.	1496
Conserver les valeurs Générateur de séquence et Normaliseur.	1496

Importation d'objets et d'objets raccourci locaux dans le même référentiel.	1497
Importation d'objets raccourci depuis un autre référentiel.	1497
Importation d'objets dans plusieurs dossiers.	1497
Importation d'objets spécifiques.	1498
Réutilisation et remplacement d'objets dépendants.	1498
Remplacement de mappages non valides.	1499
Changement de nom d'objets.	1499
Copie de mappages SAP et d'informations du programme SAP.	1500
Application d'attributs de connexion par défaut.	1500
Résolution des conflits d'objets.	1500
Utilisation du fichier de contrôle de déploiement	1501
Paramètres du fichier de contrôle de déploiement.	1503
Exemples de fichiers de contrôle de déploiement.	1507
Déploiement de la dernière version d'un dossier.	1508
Déploiement de la dernière version d'un groupe de déploiement.	1508
Création de liste de plusieurs dossiers source et cible	1508
Conseils d'utilisation de pmrep Files.	1509
Index.	1511

Préface

Consultez le guide *Référence des commandes Informatica®* pour plus d'informations sur les programmes et utilitaires de ligne de commande, tels que `infacmd`, `infasetup`, `pmcmd`, `pmpasswd` et `pmrep` pour gérer le domaine, les services d'application et les objets Informatica. Découvrez les descriptions, les options et les arguments des commandes. Vous pouvez effectuer une grande partie des fonctionnalités de la ligne de commande via l'outil Administrator tool et d'autres outils client.

Ressources Informatica

Informatica vous fournit toute une gamme de ressources de produits via Informatica Network et autres portails en ligne. Utilisez ces ressources pour tirer le meilleur parti de vos produits et solutions Informatica, et pour apprendre d'autres utilisateurs et experts en la matière d'Informatica.

Informatica Network

Informatica Network est la passerelle à de nombreuses ressources, y compris la base de connaissances Informatica et le support client international Informatica. Pour accéder à Informatica Network, visitez le site <https://network.informatica.com>.

En tant que membre d'Informatica Network, vous disposez des options suivantes :

- Rechercher les ressources de produits dans la base de connaissances.
- Afficher les informations de disponibilité des produits.
- Créer et vérifier vos dossiers de support.
- Rechercher votre réseau de groupe d'utilisateurs local Informatica et collaborer avec vos pairs.

Base de connaissances Informatica

Utilisez la base de connaissances Informatica pour rechercher des ressources de produits telles que des articles pratiques, des meilleures pratiques, des didacticiels vidéo et des questions fréquemment posées.

Pour rechercher dans la base de connaissances, visitez le site <https://search.informatica.com>. N'hésitez pas à contacter l'équipe Base de connaissances Informatica à l'adresse KB_Feedback@informatica.com pour lui faire part de vos questions, commentaires ou suggestions concernant la base de connaissances.

Documentation Informatica

Utilisez le portail de documentation Informatica pour explorer une vaste bibliothèque de documentation pour les versions de produits actuelles et récentes. Pour explorer le portail de documentation, visitez le site <https://docs.informatica.com>.

N'hésitez pas à contacter l'équipe Documentation Informatica à l'adresse info_documentation@informatica.com pour lui faire part de vos questions, commentaires ou suggestions concernant la documentation des produits.

Matrices de disponibilité des produits Informatica

Les matrices de disponibilité des produits (PAM) indiquent les versions des systèmes d'exploitation, les bases de données et les types de source et cible de données pris en charge par une version d'un produit. Vous pouvez parcourir les PAM Informatica à l'adresse <https://network.informatica.com/community/informatica-network/product-availability-matrices>.

Informatica Velocity

Informatica Velocity est un ensemble de conseils et de meilleures pratiques développés par les services professionnels d'Informatica et basés sur les expériences réelles de centaines de projets de gestion des données. Informatica Velocity représente le savoir collectif de consultants d'Informatica qui collaborent avec des organisations du monde entier pour planifier, développer, déployer et gérer des solutions performantes de gestion des données.

Vous trouverez les ressources d'Informatica Velocity à l'adresse <http://velocity.informatica.com>. Si vous avez des questions, des commentaires ou des suggestions sur Informatica Velocity, contactez les services professionnels d'Informatica à l'adresse ips@informatica.com.

Informatica Marketplace

Informatica Marketplace est un forum dans lequel vous pouvez trouver des solutions qui permettent d'augmenter et d'améliorer vos implémentations Informatica. Exploitez les centaines de solutions de développeurs et de partenaires Informatica sur Marketplace pour améliorer votre productivité et accélérer le délai d'implémentation de vos projets. Vous trouverez Informatica Marketplace à l'adresse <https://marketplace.informatica.com>.

Support client international Informatica

Vous pouvez contacter un centre de support international par téléphone ou via le réseau Informatica.

Pour rechercher le numéro de téléphone du support client international Informatica local, visitez le site Web Informatica à l'adresse <https://www.informatica.com/services-and-training/customer-success-services/contact-us.html>.

Pour trouver des ressources de support en ligne sur le réseau Informatica, visitez le site <https://network.informatica.com> et sélectionnez l'option eSupport.

CHAPITRE 1

Programmes et utilitaires de ligne de commande

- [Présentation des programmes et utilitaires de ligne de commande, 29](#)

Présentation des programmes et utilitaires de ligne de commande

L'installation d'Informatica inclut des outils d'assistance client et des programmes et utilitaires de ligne de commande. Utilisez les programmes et utilitaires de ligne de commande pour gérer le domaine Informatica, les services d'application et les objets. Vous pouvez exécuter les programmes et utilitaires de ligne de commande sur n'importe quelle machine ayant accès au domaine Informatica.

Lorsque vous installez les services ou les clients Informatica, les programmes et utilitaires de ligne de commande sont installés par défaut. Vous pouvez aussi installer et exécuter ces programmes et ces utilitaires sur d'autres machines en installant les utilitaires Informatica.

Le tableau suivant décrit les utilitaires Informatica :

Programme de ligne de commande	Description
infacmd	Administrez le domaine Informatica ainsi que les services et processus d'applications, notamment le référentiel et les services d'intégration. Vous pouvez également utiliser infacmd pour accéder aux licences et aux événements du journal et les administrer ainsi que pour exporter et importer des objets et des comptes utilisateur.
infasetup	Administrez les domaines et les nœuds.
filemanager	Administrez les capacités de prétraitement et de surveillance des fichiers d'un écosystème cloud.

Le tableau suivant décrit les utilitaires PowerCenter® :

Programme de ligne de commande	Description
pmcmd	Gérez les flux de travail. Utilisez pmcmd pour démarrer, arrêter, planifier et surveiller les flux de travail.
pmpasswd	Cryptez les mots de passe à utiliser avec les variables d'environnement pmcmd et pmrep.
pmrep	Effectue les tâches d'administration du référentiel. Utilisez pmrep pour répertorier des objets, créer et modifier des groupes ou restaurer et supprimer des référentiels.

CHAPITRE 2

Installation et configuration des utilitaires de ligne de commande

Ce chapitre comprend les rubriques suivantes :

- [Installation et configuration des utilitaires de ligne de commande - Présentation, 31](#)
- [Installation des utilitaires de ligne de commande, 32](#)
- [Configuration des utilitaires de ligne de commande, 33](#)
- [Configuration de sécurité pour les utilitaires Informatica , 35](#)

Installation et configuration des utilitaires de ligne de commande - Présentation

Lorsque vous installez les services ou les clients Informatica, les utilitaires de ligne de commande sont installés par défaut. Vous pouvez également installer et exécuter les utilitaires de ligne de commande sur une machine sans installer les produits Informatica.

Pour installer et configurer les utilitaires de ligne commande sur une machine sans produits Informatica installés, effectuez les tâches suivantes :

- Installez les utilitaires de ligne de commande.
- Configurez les utilitaires de ligne de commande.

Avant d'exécuter les programmes de ligne de commande, vous devez configurer les variables d'environnement correspondantes. Vous devez également accorder une autorisation d'exécution sur les fichiers utilitaires aux comptes utilisateur qui exécutent les commandes.

- Configurez la sécurité pour les utilitaires de ligne de commande.

Si vous activez les communications sécurisées pour le domaine ou si celui-ci utilise l'authentification Kerberos, effectuez la configuration de sécurité sur les machines sur lesquelles vous avez installé les utilitaires de ligne de commande.

Installation des utilitaires de ligne de commande

Informatica fournit un fichier .zip distinct pour installer les utilitaires de ligne de commande sur une machine sur laquelle aucun produit Informatica n'est installé.

1. Contactez le support client international Informatica pour obtenir le fichier .zip des utilitaires de ligne de commande.
2. Extrayez les fichiers sur la machine sur laquelle vous voulez exécuter les utilitaires de ligne de commande.
3. Sous Windows, installez le package redistribuable de Microsoft Visual Studio 2013 inclus dans les fichiers extraits. Exécutez le fichier 32 ou 64 bits situé dans le répertoire suivant :

```
<répertoire d'installation des utilitaires>/PowerCenter/server/VS2013
```

Les produits Informatica sous Windows requièrent le package redistribuable de Microsoft Visual Studio 2013. Lorsque vous installez les services ou les clients Informatica, le programme d'installation installe le package redistribuable. Lorsque vous installez les utilitaires de ligne de commande autonomes, le package redistribuable est inclus dans les fichiers extraits et vous devez l'installer manuellement.

Répertoires d'installation

Les répertoires d'installation des utilitaires de ligne de commande varient selon que les utilitaires sont installés dans le cadre de l'installation des services Informatica, de l'installation du client Informatica ou de l'installation autonome des utilitaires de ligne de commande.

Installation des services Informatica

Les utilitaires Informatica sont installés dans le répertoire suivant :

```
<répertoire d'installation Informatica>/isp/bin
```

Les utilitaires PowerCenter sont installés dans le répertoire suivant :

```
<répertoire d'installation Informatica>/server/bin
```

Les utilitaires Metadata Manager sont installés dans le répertoire suivant :

```
<répertoire d'installation Informatica>/services/MetadataManagerService/utilities
```

Installation du client Informatica

Lorsque vous installez l'outil Developer, les utilitaires Informatica sont installés dans le répertoire suivant :

```
<répertoire d'installation Informatica>/clients/DeveloperClient/infacmd
```

Lorsque vous installez le client PowerCenter, les utilitaires PowerCenter sont installés dans le répertoire suivant :

```
<répertoire d'installation Informatica>/clients/PowerCenterClient/  
CommandLineUtilities/PC/server/bin
```

Lorsque vous installez le client PowerCenter, les utilitaires Metadata Manager sont installés dans le répertoire suivant :

```
<répertoire d'installation Informatica>/clients/PowerCenterClient/CommandLineUtilities/MM
```

Installation des utilitaires de ligne de commande

Les utilitaires Informatica sont installés dans le répertoire suivant :

<répertoire d'installation des utilitaires>/PowerCenter/isp/bin

Les utilitaires PowerCenter sont installés dans le répertoire suivant :

<répertoire d'installation des utilitaires>/PowerCenter/server/bin

Les utilitaires Metadata Manager sont installés dans le répertoire suivant :

<répertoire d'installation des utilitaires>/MetadataManager/utilities

Configuration des utilitaires de ligne de commande

Configurez le chemin et les variables d'environnement comme l'exigent les utilitaires de ligne de commande. Accordez l'autorisation d'exécution sur les fichiers utilitaires aux comptes utilisateur qui exécutent les commandes.

Configurer les utilitaires Informatica

Configurez les variables d'environnement requises pour les programmes de ligne de commande infacmd et infasetup.

Pour exécuter infacmd, définissez la variable d'environnement ICMD_JAVA_OPTS.

Pour exécuter infasetup, définissez la variable d'environnement INFA_JAVA_CMD_OPTS.

Configurer les utilitaires PowerCenter

Avant d'exécuter les utilitaires PowerCenter, utilisez les directives suivantes pour configurer les fichiers de programme et les variables :

- Pour exécuter pmrep, pmcmd et pmpasswd, copiez le fichier domains.infa du domaine Informatica dans le répertoire des utilitaires.
- Pour exécuter pmrep, pmcmd et pmpasswd sous UNIX, définissez INFA_HOME, PATH et les variables d'environnement de bibliothèque partagée sur l'emplacement des utilitaires.

Par exemple, si les utilitaires de ligne de commande sont installés dans le dossier /data/Informatica_cmd_utilities/, les utilitaires PowerCenter se trouvent dans le dossier /data/Informatica_cmd_utilities/PowerCenter/server/bin. Sous Linux, vous pouvez définir les variables d'environnement à l'invite de commande comme suit :

```
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
```

Remarque: Redémarrez la machine après avoir configuré INFA_HOME ou la variable d'environnement de bibliothèque partagée.

Configurer les utilitaires Metadata Manager

Pour configurer les utilitaires Metadata Manager, configurez les variables d'environnement qui spécifient l'emplacement de la machine virtuelle Java et le répertoire racine Informatica.

Si le domaine utilise l'authentification Kerberos, créez le fichier domains.infa. Les programmes de ligne de commande de Metadata Manager utilisent le fichier domains.infa pour obtenir des informations de connectivité de passerelle pour le domaine.

Configurez les variables d'environnement suivantes :

JAVA_HOME

Spécifie l'emplacement de la machine virtuelle Java. Définissez JAVA_HOME sur le répertoire Java de PowerCenter pendant l'installation des utilitaires de ligne de commande. Par exemple :

```
<répertoire d'installation des utilitaires>\PowerCenter\Java
```

Définissez cette variable d'environnement dans chaque programme de ligne de commande Metadata Manager comme suit :

1. Ouvrez le fichier par lots ou le script shell avec un éditeur de texte.
2. Recherchez la ligne qui définit JAVA_HOME sur @INFA_JDK_HOME@.
3. Remplacez la chaîne @INFA_JDK_HOME@ par le répertoire Java de PowerCenter. Par exemple :

```
set JAVA_HOME=C:\InfaUtilities\PowerCenter\java
```
4. Enregistrez et fermez le fichier par lots ou le script shell.

INFA_HOME

Spécifie le répertoire racine d'Informatica afin que les applications et les services Informatica puissent trouver les autres composants Informatica dont ils ont besoin pour s'exécuter. Définissez INFA_HOME en fonction du répertoire PowerCenter dans l'installation des utilitaires de ligne de commande. Par exemple :

```
<répertoire d'installation des utilitaires>\PowerCenter
```

Définissez cette variable d'environnement sur chaque machine sur laquelle vous avez installé les utilitaires Informatica.

Remarque: Redémarrez la machine après avoir configuré le répertoire INFA_HOME.

Créer le fichier domains.infa

Le fichier domains.infa contient les informations de connectivité de passerelle du domaine. Lorsque le domaine utilise l'authentification Kerberos, créez le fichier domains.infa pour que les programmes de ligne de commande puissent obtenir les informations de connectivité de passerelle du domaine.

Si le domaine utilise l'authentification Kerberos, vous devez entrer les informations de connectivité du domaine lorsque vous exécutez les commandes des programmes de ligne de commande. Entrez les informations de connectivité du domaine via l'option --domainName ou --gateway. Vous ne pouvez utiliser l'option --domainName que si le fichier domains.infa contient les informations de connectivité de passerelle du domaine. Si le fichier domains.infa n'existe pas ou si ses informations sont obsolètes, vous devez utiliser l'option --gateway lorsque vous exécutez une commande de connexion au domaine.

Lorsque vous installez les services Informatica, le fichier domains.infa est disponible dans le répertoire INFA_HOME. Pour toute autre installation, créez le fichier et vérifiez qu'il est disponible sur la machine à partir de laquelle vous voulez exécuter les commandes.

Pour créer le fichier domains.infa, exécutez la commande `infacmd isp UpdateGatewayInfo`. La commande crée ou met à jour le fichier domains.infa dans le répertoire PowerCenter de l'installation des utilitaires de ligne de commande, par exemple `<répertoire d'installation des utilitaires>\PowerCenter`.

Configuration de sécurité pour les utilitaires Informatica

Lors de l'installation des utilitaires Informatica, vous devrez peut-être configurer les machines en fonction de la configuration de sécurité du domaine. Si vous ne configurez pas les machines correctement, les programmes de ligne de commande ne pourront peut-être pas authentifier les utilisateurs avec le domaine.

Configurez les machines sur lesquelles vous avez installé les utilitaires Informatica lorsque le domaine utilise les configurations de sécurité suivantes :

Communication sécurisée

Si la communication sécurisée est activée pour le domaine, vous devrez peut-être configurer les machines pour utiliser le fichier truststore. Si vous utilisez un fichier truststore personnalisé, vous devez configurer les variables d'environnement qui indiquent le répertoire du fichier truststore et le mot de passe truststore.

Authentification Kerberos

Si le domaine utilise l'authentification Kerberos, vous devez copier le fichier de configuration Kerberos sur les machines sur lesquelles vous avez installé les utilitaires Informatica. Vous devez aussi configurer les machines pour localiser le fichier de configuration Kerberos pour le domaine.

LIENS CONNEXES :

- [“ Exécution de commandes dans un domaine sécurisé ” à la page 39](#)
- [“ Exécution de commandes sous UNIX avec l'authentification Kerberos ” à la page 40](#)
- [“ Exécution de commandes sous Windows avec l'authentification Kerberos ” à la page 42](#)

CHAPITRE 3

Utilisation des programmes de ligne de commande

Ce chapitre comprend les rubriques suivantes :

- [Présentation de l'utilisation des programmes de ligne de commande, 36](#)
- [Entrée d'options et d'arguments, 37](#)
- [Notation de syntaxe, 38](#)
- [Exécution de commandes dans un domaine sécurisé, 39](#)
- [Exécution de commandes sous UNIX avec l'authentification Kerberos, 40](#)
- [Exécution de commandes sous Windows avec l'authentification Kerberos, 42](#)

Présentation de l'utilisation des programmes de ligne de commande

Informatica comprend des programmes de ligne de commande que vous utilisez pour effectuer des tâches depuis n'importe quelle machine de l'environnement Informatica. Les programmes de ligne de commande vous permettent d'exécuter un sous-ensemble de tâches que vous pouvez effectuer dans Informatica Administrator.

Par exemple, vous pouvez activer ou désactiver un service de référentiel depuis l'outil Administrator ou depuis le programme de ligne de commande `infacmd`.

Informatica comprend les programmes de ligne de commande suivants :

- **infacmd**. Utilisez `infacmd` pour accéder aux services d'application Informatica.
- **infacmd**. Utilisez `infacmd` pour obtenir le nom de nœud, mettre à jour les informations de passerelle et répertorier les plug-in de prise en charge.
- **infasetup**. Utilisez la commande `infasetup` pour effectuer des tâches d'installation telles que la définition d'un nœud ou d'un domaine.
- **infasetup**. Utilisez la commande `infasetup` pour mettre à jour le nœud de passerelle.
- **pmcmd**. Utilisez `pmcmd` pour gérer les flux de travail. Vous pouvez démarrer, arrêter, planifier et contrôler les flux de travail en utilisant `pmcmd`.
- **pmrep**. Utilisez `pmrep` pour effectuer des tâches d'administration du référentiel telles que la liste des objets du référentiel, la création et l'édition des groupes et la restauration et la suppression des référentiels.

- **mmcmd.** Utilisez la commande mmcmd pour charger et gérer les ressources ainsi que pour importer et exporter des modèles et des ressources personnalisées.
- **mmLineageMigrator.** Utilisez mmlineagemigrator pour migrer les informations de liaison de lignage des données après la mise à niveau depuis Metadata Manager 9.6.x vers la version actuelle.
Remarque: L'exécution de ce programme est automatique ; vous n'avez pas à l'exécuter, sauf si la migration échoue et que vous corrigez l'erreur ou si le support client international Informatica vous y invite.
- **mmRepoCmd.** Utilisez la commande mmRepoCmd pour créer, supprimer, sauvegarder et restaurer le contenu du référentiel Metadata Manager. Vous pouvez également restaurer un fichier de sauvegarde du référentiel PowerCenter contenant les objets Metadata Manager dans la base de données du référentiel PowerCenter.
- **mmXConPluginUtil.** Utilisez mmxconpluginutil pour générer les informations de mappage de l'image ou le plug-in pour une connexion XConnect universelle.
- **rcfmu.** Utilisez rcfmu pour migrer un fichier de configuration de ressource d'une version précédente de Metadata Manager vers la version actuelle.
- **rmu.** Utilisez rmu pour migrer les ressources d'une version précédente de Metadata Manager vers la version actuelle.

Pour exécuter les programmes de ligne de commande sous UNIX, vous devrez peut-être définir la variable d'environnement du chemin de la bibliothèque à l'emplacement des utilitaires Informatica.

Pour faciliter l'utilisation, vous pouvez configurer les variables d'environnement qui s'appliquent chaque fois que vous exécutez les programmes de ligne de commande.

Par exemple, vous pouvez définir une variable d'environnement pour le nom de domaine par défaut, l'utilisateur et le mot de passe pour éviter de saisir les options dans la ligne de commande.

Par exemple, vous pouvez définir une variable d'environnement pour le nom de domaine par défaut et l'utilisateur pour éviter de saisir les options dans la ligne de commande.

Entrée d'options et d'arguments

Chaque programme de ligne de commande requiert un ensemble d'options et d'arguments. Ceux-ci incluent le nom d'utilisateur, le mot de passe, le nom de domaine et les informations de connexion.

Utilisez les règles suivantes lorsque vous entrez des options et arguments de commande :

- Pour entrer des options, saisissez un trait d'union suivi d'une lettre, deux lettres ou un mot, selon la syntaxe du programme de la commande.
Par exemple, la commande de connexion pmrep utilise une option d'une seule lettre pour le nom du référentiel :

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

- Entrez les options dans n'importe quel ordre.
- Si une option que vous spécifiez depuis la ligne de commande contient des espaces, placez l'option entre guillemets doubles.
- Le premier mot après l'option est l'argument.
- La plupart des options requièrent des arguments.
Vous devez séparer les options des arguments avec un espace unique lorsque vous utilisez pmcmd ou infacmd. Vous ne devez pas séparer les options des arguments lorsque vous utilisez pmrep.

Vous devez séparer les options des arguments avec un espace unique lorsque vous utilisez infacmd.

- Si un argument contient plus d'un mot, placez l'argument entre guillemets doubles.

Pour pmrep et pmcmd, vous pouvez également utiliser des guillemets simples.

Les guillemets non correspondants entraînent une erreur.

Pour infacmd ou pmcmd, les programmes de ligne de commande ignorent les guillemets qui n'entourent pas un argument.

Pour infacmd, les programmes de ligne de commande ignorent les guillemets qui n'entourent pas un argument.

- Si un argument est au format `option_name=value` et si la valeur contient un espace et un signe égal (=), assurez-vous qu'une barre oblique inversée précède le signe d'égalité.
Par exemple, un argument contient l'option `DatabaseUser` et le nom d'utilisateur de base de données est `a#v%5^=! !`. Utilisez le format suivant lorsque vous entrez l'argument : `DBUser=a#v%5^\=! !`
- Pour mettre à jour les valeurs des options de connexion avec les variables d'environnement existantes, utilisez un caractère d'échappement devant tout signe dollar (\$) avec n'importe quel interpréteur de commandes autre que CSH.
- Pour pmrep, vous pouvez utiliser des espaces dans un argument. Pour spécifier un argument contenant des espaces, entourez-le de guillemets simples ou doubles. Lorsque vous utilisez des guillemets simples ou doubles dans l'argument, assurez-vous qu'une barre oblique inversée précède les guillemets requis.

Notation de syntaxe

Le tableau suivant décrit la notation utilisée dans ce livre pour afficher la syntaxe de tous les programmes de ligne de commande Informatica :

Convention	Description
-x	Option placée avant un argument. Ceci désigne le paramètre que vous entrez. Par exemple, pour entrer le nom d'utilisateur pour pmcmd, tapez -u ou -user suivi du nom d'utilisateur.
< x >	Option obligatoire. Si vous omettez une option obligatoire, le programme de ligne de commande renvoie un message d'erreur.
<x y > {x y}	Sélectionnez une des options requises. Pour que la commande s'exécute, vous devez sélectionner une des options suivantes. Si vous omettez une option obligatoire, le programme de ligne de commande renvoie un message d'erreur. Dans pmrep, des accolades désignent des groupements d'options obligatoires, comme dans l'exemple suivant : <pre>KillUserConnection { -i <connection_id> -n <user_name> -a (kill_all) }</pre> Si une barre droite () sépare les options, vous devez spécifier une et une seule option. Si les options ne sont pas séparées par des barres droites, vous devez spécifier toutes les options.

Convention	Description
[x]	<p>Paramètre facultatif. La commande s'exécute que vous entriez les paramètres facultatifs ou non. Par exemple, la commande Help a la syntaxe suivante :</p> <p>Help [Command]</p> <p>Si vous entrez une commande, le programme de ligne de commande renvoie seulement des informations sur cette commande. Si vous omettez le nom de commande, le programme de ligne de commande renvoie une liste de toutes les commandes.</p>
[x y]	<p>Sélectionnez un des paramètres facultatifs.</p> <p>Par exemple, plusieurs commandes dans pmcmd s'exécutent soit en mode wait, soit en mode nowait.</p> <p>[-wait -nowait]</p> <p>Si vous spécifiez un mode, la commande s'exécute dans le mode spécifié. La commande s'exécute, que vous entriez les paramètres facultatifs ou non.</p> <p>Si vous ne spécifiez pas un mode, pmcmd exécute la commande dans le mode nowait par défaut.</p>
< < x y> <a b> >	<p>Quand un ensemble contient des sous-ensembles, le surensemble est indiqué avec des parenthèses en gras < > .</p> <p>Une barre droite en gras () sépare les sous-ensembles.</p>
(text)	<p>Dans pmrep, des parenthèses entourent un texte descriptif, comme la liste des valeurs possibles pour un argument ou une explication pour une option qui ne prend pas d'argument.</p> <p>Des parenthèses entourent un texte descriptif, comme la liste des valeurs possibles pour un argument ou une explication pour une option qui ne prend pas d'argument.</p>

Exécution de commandes dans un domaine sécurisé

Si le domaine Informatica dispose d'une communication sécurisée activée, vous devez définir les variables d'environnement sur la machine qui héberge les programmes de ligne de commande pour exécuter les commandes de manière sécurisée. Vous devez définir les variables d'environnement avant d'exécuter les commandes infacmd, pmrep, mmcmd, mmRepoCmd et pmcmd.

Définissez les variables d'environnement suivantes avant d'exécuter les commandes :

INFA_TRUSTSTORE

Définissez la variable d'environnement INFA_TRUSTSTORE avec le répertoire qui contient les fichiers truststore pour les certificats SSL. Le répertoire doit contenir les fichiers truststore nommés infa_truststore.jks et infa_truststore.pem. Vous devez définir la variable INFA_TRUSTSTORE si vous utilisez le certificat SSL par défaut depuis Informatica ou si vous spécifiez un certificat SSL.

INFA_TRUSTSTORE_PASSWORD

Si vous spécifiez le certificat SSL pour activer la communication sécurisée dans le domaine, définissez la variable d'environnement INFA_TRUSTSTORE_PASSWORD avec le mot de passe avec le mot de passe pour le fichier infa_truststore.jks qui contient le certificat SSL. Vous n'avez pas besoin de définir cette variable si vous utilisez le certificat SSL par défaut depuis Informatica.

Remarque: Le mot de passe doit être crypté. Utilisez le programme de ligne de commande `pmpasswd` pour crypter le mot de passe avec le type de cryptage `CRYPT_SYSTEM`. Pour plus d'informations, voir ["Chiffrement des mots de passe" à la page 61](#).

Exécution de commandes sous UNIX avec l'authentification Kerberos

Si le domaine Informatica utilise l'authentification Kerberos, définissez la variable d'environnement de configuration Kerberos avant d'exécuter les programmes de ligne de commande. Si vous exécutez les programmes de ligne de commande avec l'authentification unique, vous devez générer un fichier cache de justificatifs d'identité et spécifier le chemin et le nom de fichier dans une variable d'environnement.

Vous devez définir les variables d'environnement avant d'exécuter les commandes `infacmd`, `pmrep`, `mmcmd`, `mmRepoCmd` et `pmcmd` sous UNIX.

Exécution de commandes sous UNIX avec l'authentification unique

Si vous exécutez les programmes de ligne de commande avec l'authentification unique, vous devez générer un fichier cache de justificatifs d'identité pour authentifier le compte utilisateur exécutant les commandes sur le réseau Kerberos. Utilisez l'utilitaire *kinit* pour générer le fichier cache de justificatifs d'identité.

Si vous disposez d'un fichier cache de justificatifs d'identité, vous pouvez exécuter les commandes sans les options nom d'utilisateur et mot de passe.

Pour exécuter des commandes sous UNIX avec l'authentification unique, effectuez les tâches suivantes :

1. Définissez les variables d'environnement Kerberos.
2. Téléchargez l'utilitaire *kinit* et générez un fichier cache de justificatifs d'identité.

Paramétrage des variables d'environnement Kerberos

Sur la machine qui héberge les programmes de ligne de commande, spécifiez l'emplacement du cache de justificatifs d'identité et le fichier de configuration dans les variables d'environnement Kerberos.

Définissez les variables d'environnement suivantes :

KRB5CCNAME

Stocke le chemin par défaut et le nom de fichier pour le cache de justificatifs d'identité Kerberos. Lorsque vous exécutez l'utilitaire *kinit* pour générer le cache de justificatifs d'identité utilisateur, *kinit* stocke le cache de justificatifs d'identité dans le fichier par défaut que vous avez défini dans la variable d'environnement `KRB5CCNAME`.

KRB5_CONFIG

Stocke le chemin et nom du fichier de configuration Kerberos. Le nom du fichier de configuration Kerberos est `krb5.conf`. Pour plus d'informations sur le contenu du fichier `krb5.conf`, consultez le *Guide de sécurité d'Informatica*.

Génération du fichier cache de justificatifs d'identité

Utilisez l'utilitaire Kerberos *kinit* pour générer le fichier cache de justificatifs d'identité pour le compte utilisateur qui exécute les programmes de ligne de commande. L'utilitaire est disponible avec le package de téléchargement MIT Kerberos V5.

Pour générer le fichier cache de justificatifs d'identité, effectuez les tâches suivantes :

1. Téléchargez et installez MIT Kerberos V5.

Vous pouvez télécharger MIT Kerberos V5 sur le site Web suivant : <http://web.mit.edu/Kerberos/dist/#krb5-1.12>

2. Exécutez l'utilitaire *kinit* et spécifiez le nom principal de l'utilisateur.

Lorsque vous créez le cache d'informations d'identification de l'utilisateur, vous devez utiliser l'option forwardable (-f). Vous pouvez utiliser la syntaxe de commande suivante :

```
kinit -f <principal name>
```

Le format pour le nom principal est <username>@<realmname.com>. Entrez le nom du domaine en lettres majuscules.

Remarque: Si vous définissez la variable d'environnement *KRB5CCNAME* avant d'exécuter l'utilitaire *kinit*, *kinit* stocke le cache de justificatifs d'identité à l'emplacement spécifié dans la variable d'environnement.

3. Entrez le mot de passe pour le compte d'utilisateur.

Exécution de commandes sous UNIX sans l'authentification unique

Pour exécuter des commandes sous UNIX sans l'authentification unique, définissez la variable d'environnement *KRB5_CONFIG* pour le chemin et le nom du fichier de configuration Kerberos. Incluez le nom d'utilisateur et le mot de passe lorsque vous exécutez la commande ou définissez le nom d'utilisateur et le mot de passe dans les variables d'environnement.

Les commandes déterminent les justificatifs d'identité de l'utilisateur en fonction de la manière dont vous spécifiez le nom d'utilisateur et mot de passe. Les commandes vérifient les justificatifs d'identité dans l'ordre suivant :

1. Options de commande. Si vous incluez l'option nom d'utilisateur (-un) et l'option mot de passe (-pd) dans la commande, celle-ci utilise le nom d'utilisateur et le mot de passe spécifiés pour les options.

Si un domaine Kerberos unique est utilisé pour l'authentification, spécifiez l'élément *SamAccountName* pour l'utilisateur comme option Nom d'utilisateur. Si le domaine utilise l'authentification inter-domaines Kerberos, spécifiez le nom du principal de l'utilisateur comme valeur pour l'option Nom d'utilisateur.

2. Variables d'environnement. Si vous n'incluez pas les options nom d'utilisateur et mot de passe dans la commande, celle-ci utilise le nom d'utilisateur et le mot de passe spécifiés dans les variables d'environnement *INFA_DEFAULT_DOMAIN_USER* et *INFA_DEFAULT_DOMAIN_PASSWORD*.

Remarque: Si vous ne définissez pas les justificatifs d'identité dans les options de commande ou les variables d'environnement, la commande recherche un fichier cache de justificatifs d'identité. Si un cache de justificatifs d'identité est disponible, la commande s'exécute avec l'authentification unique.

Exécution de commandes sous Windows avec l'authentification Kerberos

Sous Windows, les commandes `infacmd`, `pmrep`, `mmcmmcmd`, `mmRepoCmd` et `pmcmd` utilisent les justificatifs d'identité connectés pour l'authentification unique. Vous n'avez pas à générer un fichier cache de justificatifs d'identité.

Si vous n'utilisez pas l'authentification unique sous Windows, définissez la variable d'environnement `KRB5_CONFIG` sur le chemin et le nom de fichier de configuration Kerberos. Le nom du fichier de configuration est `krb5.conf`.

Les commandes déterminent les justificatifs d'identité de l'utilisateur en fonction de la manière dont vous spécifiez le nom d'utilisateur et mot de passe. Les commandes vérifient les justificatifs d'identité dans l'ordre suivant :

1. Options de commande. Si vous incluez l'option nom d'utilisateur (`-un`) et l'option mot de passe (`-pd`) dans la commande, celle-ci utilise le nom d'utilisateur et le mot de passe spécifiés pour les options.
Si un domaine Kerberos unique est utilisé pour l'authentification, spécifiez l'élément `samAccountName` pour l'utilisateur comme option Nom d'utilisateur. Si le domaine utilise l'authentification inter-domaines Kerberos, spécifiez le nom du principal de l'utilisateur comme valeur pour l'option Nom d'utilisateur.
2. Variables d'environnement. Si vous n'incluez pas les options nom d'utilisateur et mot de passe dans la commande, celle-ci utilise le nom d'utilisateur et le mot de passe spécifiés dans les variables d'environnement `INFA_DEFAULT_DOMAIN_USER` et `INFA_DEFAULT_DOMAIN_PASSWORD`.

Remarque: Si vous ne définissez pas les justificatifs d'identité dans les options de commande ou les variables d'environnement, la commande utilise les justificatifs d'identité connectés et exécute la commande avec l'authentification unique.

CHAPITRE 4

Variables d'environnement pour les programmes de ligne de commande

Ce chapitre comprend les rubriques suivantes :

- [Présentation des variables d'environnement pour les programmes de ligne de commande, 44](#)
- [ICMD_JAVA_OPTS, 46](#)
- [INFA_CLIENT_RESILIENCE_TIMEOUT, 46](#)
- [INFA_CODEPAGENAME, 47](#)
- [INFA_DEFAULT_DATABASE_PASSWORD, 48](#)
- [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](#)
- [Chiffrement des mots de passe, 61](#)
- [Définition du nom d'utilisateur, 63](#)

Présentation des variables d'environnement pour les programmes de ligne de commande

Vous pouvez configurer des variables d'environnement facultatives pour les programmes de ligne de commande. Par exemple, vous pouvez définir des variables d'environnement pour crypter les mots de passe, configurer les options d'affichage des dates et des heures ou encore stocker les informations de connexion par défaut pour un domaine.

Si vous exécutez les commandes `pmcmd` ou `pmrep` en mode interactif, vous devez quitter le programme de ligne de commande et vous reconnecter pour utiliser les nouvelles variables d'environnement.

Sous Windows, vous pouvez configurer ces variables d'environnement comme variables utilisateur ou comme variables système. Pour plus d'informations sur le paramétrage des variables d'environnement sous Windows, consultez la documentation Windows.

Remarque: Les variables d'environnement que vous configurez s'appliquent aux programmes de ligne de commande exécutés sur le nœud. Pour appliquer les modifications, redémarrez le nœud.

Le tableau suivant décrit les variables d'environnement que vous pouvez configurer pour une utilisation avec les programmes de ligne de commande :

Variable d'environnement	Programmes de ligne de commande	Description
ICMD_JAVA_OPTS	infacmd	Définit les options Java.
INFA_CLIENT_RESILIENCE_TIMEOUT	infacmd pmcmd pmrep	Limite le nombre de secondes attribuées aux programmes de ligne de commande pour l'établissement d'une connexion au domaine ou au service.
INFA_CODEPAGE_NAME	pmcmd pmrep	Configure le jeu de caractères utilisé par <i>pmcmd</i> et <i>pmrep</i> .
INFA_DEFAULT_CONNECTION_PASSWORD	infacmd	Stocke le mot de passe du fichier truststore de base de données pour la base de données sécurisée.
INFA_DEFAULT_DATABASE_PASSWORD	infasetup	Stocke le mot de passe utilisateur par défaut pour la base de données de configuration du domaine.
INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD	infasetup	Stocke le mot de passe truststore de la base de données.
INFA_DEFAULT_DOMAIN	infacmd pmcmd pmrep	Stocke le nom de domaine par défaut.
INFA_DEFAULT_DOMAIN_PASSWORD	infacmd	Stocke le mot de passe utilisateur par défaut du domaine.
INFA_DEFAULT_DOMAIN_USER	infacmd	Stocke le nom d'utilisateur par défaut du domaine.

Variable d'environnement	Programmes de ligne de commande	Description
INFA_DEFAULT_PWX_OSEPASSWORD	infacmd pwx	Stocke un mot de passe chiffré pour le système d'exploitation.
INFA_DEFAULT_PWX_OSPASSWORD	infacmd pwx	Stocke un mot de passe en texte clair pour le système d'exploitation.
INFA_DEFAULT_SECURITY_DOMAIN	infacmd	Stocke le domaine de sécurité pour l'authentification LDAP.
INFA_DOMAINS_FILE	infacmd infasetup pmcmd pmrep	Stocke le chemin et le nom du fichier domains.infa.
INFA_JAVA_CMD_OPTS	infasetup	Définit les options Java.
INFA_NODE_KEYSTORE_PASSWORD	infasetup	Stocke le mot de passe du fichier infa_keystore.jks.
INFA_NODE_TRUSTSTORE_PASSWORD	infasetup	Stocke le mot de passe du fichier infa_truststore.jks.
INFA_PASSWORD	infacmd	Stocke le mot de passe par défaut de l'utilisateur.
INFA_REPCNX_INFO	pmrep	Stocke le nom du fichier de connexion du référentiel.
INFA_REPOSITORY_PASSWORD	infacmd	Stocke le mot de passe par défaut de l'utilisateur du référentiel PowerCenter.
INFATool_DATEFORMAT	pmcmd	Configure la manière dont pmcmd affiche la date et l'heure.
<Password_Environment_Variable>	pmcmd pmrep	Chiffre et stocke le mot de passe.
<User_Name_Environment_Variable>	pmcmd pmrep	Stocke le nom d'utilisateur.

LIENS CONNEXES :

- ["Chiffrement des mots de passe" à la page 61](#)
- ["Définition du nom d'utilisateur" à la page 63](#)

ICMD_JAVA_OPTS

La variable d'environnement ICMD_JAVA_OPTS s'applique au programme de ligne de commande infacmd.

Vous pouvez configurer la variable d'environnement ICMD_JAVA_OPTS pour définir les options Java telles que les valeurs -Xmx et les propriétés système. Pour définir une propriété système, passez la valeur au format suivant :

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

Par exemple, vous pouvez avoir besoin d'augmenter la mémoire système utilisée par infacmd. La mémoire système par défaut pour infacmd est 512 Mo. Pour configurer une mémoire de 1024 Mo dans un environnement C shell UNIX, entrez :

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

Configuration d'ICMD_JAVA_OPTS sous UNIX

Pour configurer ICMD_JAVA_OPTS sous UNIX :

- Dans un environnement de shell C UNIX, saisissez :

```
setenv ICMD_JAVA_OPTS <Java_Options>
```

Dans un environnement de shell Bourne UNIX, saisissez :

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

Configuration d'ICMD_JAVA_OPTS sous Windows

Pour configurer ICMD_JAVA_OPTS sous Windows :

- Entrez la variable d'environnement ICMD_JAVA_OPTS et définissez les options Java telles que les valeurs -Xmx et les propriétés système.

Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

INFA_CLIENT_RESILIENCE_TIMEOUT

La variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT s'applique aux programmes de ligne de commande infacmd, pmcmd et pmrep.

Vous pouvez paramétrer la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT pour limiter le nombre de secondes attribuées aux programmes de ligne de commande pour l'établissement de connexions au domaine ou au service. Le temps par défaut est 180 secondes si vous ne paramétrez pas la variable d'environnement.

Configuration d'INFA_CLIENT_RESILIENCE_TIMEOUT sous UNIX

Pour configurer INFA_CLIENT_RESILIENCE_TIMEOUT sous UNIX :

- Dans un environnement de shell C UNIX, saisissez :

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

Dans un environnement de shell Bourne UNIX, saisissez :

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

Configuration d'INFA_CLIENT_RESILIENCE_TIMEOUT sous Windows

Pour configurer INFA_CLIENT_RESILIENCE_TIMEOUT sous Windows :

- Entrez la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT et définissez la valeur en fonction du nombre de secondes que vous souhaitez attribuer aux programmes de ligne de commande pour l'établissement d'une connexion au domaine ou au service.

Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

INFA_CODEPAGENAME

La variable d'environnement INFA_CODEPAGENAME s'applique aux programmes de ligne de commande *pmcmd* et *pmrep*.

pmcmd et *pmrep* envoient des commandes Unicode et utilisent la page de code de la machine hôte sauf si vous paramétrez la page de code de la variable d'environnement INFA_CODEPAGENAME pour la remplacer. Si vous définissez INFA_CODEPAGENAME de *pmcmd*, la page de code doit être compatible avec la page de code du service d'intégration. Si vous définissez INFA_CODEPAGENAME de *pmrep*, la page de code doit être compatible avec la page de code du référentiel. Si vous définissez INFA_CODEPAGENAME sur la machine qui exécute la commande *pmcmd* et *pmrep*, la page de code doit être compatible avec les pages de code du service d'intégration et du référentiel.

Si les pages de code ne sont pas compatibles, la commande peut échouer.

Configuration d'INFA_CODEPAGENAME sous UNIX

Pour configurer INFA_CODEPAGENAME sous UNIX :

- Dans un environnement de shell C UNIX, saisissez :

```
setenv INFA_CODEPAGENAME <code page name>
```

Dans un environnement de shell Bourne UNIX, saisissez :

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

Configuration d'INFA_CODEPAGE_NAME sous Windows

Pour configurer INFA_CODEPAGE_NAME sous Windows :

- Entrez la variable d'environnement INFA_CODEPAGE_NAME et définissez la valeur du nom de la page de code.

Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

INFA_DEFAULT_DATABASE_PASSWORD

La variable d'environnement INFA_DEFAULT_DATABASE_PASSWORD s'applique au programme de ligne de commande *infasetup*.

Certaines commandes *infasetup* exigent un mot de passe de la base de données de configuration du domaine. Vous pouvez indiquer ce mot de passe dans l'option de la commande *infasetup* ou vous pouvez le stocker dans la variable d'environnement INFA_DEFAULT_DATABASE_PASSWORD.

Suivez la procédure suivante pour utiliser un mot de passe crypté comme variable d'environnement :

1. Utilisez le programme de ligne de commande *pmpasswd* pour crypter le mot de passe utilisateur.
pmpasswd génère et affiche le mot de passe crypté. Par exemple, si vous entrez le mot de passe « lundi », il sera crypté et deviendra f/wRb5PZsZnqESTDPeos7Q==.
2. Configurez la variable d'environnement de mot de passe pour définir la valeur cryptée.

LIENS CONNEXES :

- [“Chiffrement des mots de passe” à la page 61](#)

Configuration d'INFA_DEFAULT_DATABASE_PASSWORD sous UNIX

Pour configurer INFA_DEFAULT_DATABASE_PASSWORD sous UNIX :

1. À la ligne de commande, saisissez :

```
pmpasswd <database password>
```

pmpasswd renvoie le mot de passe crypté.

2. Dans un environnement de shell C UNIX, saisissez :

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

Dans un environnement de shell Bourne UNIX, saisissez :

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

Configuration d'INFA_DEFAULT_DATABASE_PASSWORD sous Windows

Pour configurer INFA_DEFAULT_DATABASE_PASSWORD sous Windows :

1. À la ligne de commande, saisissez :

```
pmpasswd <database password>
```

pmpasswd renvoie le mot de passe crypté.

2. Entrez la variable d'environnement INFA_DEFAULT_DATABASE_PASSWORD et définissez la valeur du mot de passe *crypté*.

Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD

La variable d'environnement INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD s'applique au programme de ligne de commande infasetup.

Certaines commandes *infasetup* configurent la communication sécurisée pour le domaine. Vous pouvez fournir le mot de passe du fichier truststore de la base de données sécurisée en tant qu'option avec *infasetup* ou le stocker en tant que variable d'environnement

INFA_DEFAULT_DB_TRUSTSTORE_DATABASE_PASSWORD.

Suivez la procédure suivante pour utiliser un mot de passe crypté comme variable d'environnement :

1. Utilisez le programme de ligne de commande *pmpasswd* pour crypter le mot de passe utilisateur.

pmpasswd génère et affiche le mot de passe crypté. Par exemple, si vous entrez le mot de passe « lundi », il sera crypté et deviendra f/wRb5PZsZnqESTDPeos7Q==.

2. Configurez la variable d'environnement de mot de passe pour définir la valeur cryptée.

Configuration de INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD sous UNIX

Pour configurer INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD sous UNIX :

1. Sur la ligne de commande, saisissez :

```
pmpasswd <database password>
```

pmpasswd renvoie le mot de passe crypté.

2. Dans un environnement de shell C UNIX, saisissez :

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

Dans un environnement de shell Bourne UNIX, saisissez :

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

Configuration de INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD sous Windows

Pour configurer INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD sous Windows :

1. Sur la ligne de commande, saisissez :

```
pmpasswd <database password>
```

pmpasswd renvoie le mot de passe crypté.

2. Entrez la variable d'environnement INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD et définissez la valeur sur le mot de passe crypté.

Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

INFA_DEFAULT_DOMAIN

La variable d'environnement INFA_DEFAULT_DOMAIN s'applique aux programmes de ligne de commande infacmd, pmcmd et pmrep.

Les programmes de ligne de commande requièrent un nom de domaine. Vous pouvez fournir le nom de domaine dans une option des programmes de ligne de commande ou vous pouvez le stocker dans la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous avez plus d'un domaine, sélectionnez un domaine par défaut.

Configuration d'INFA_DEFAULT_DOMAIN sous UNIX

Pour configurer INFA_DEFAULT_DOMAIN sous UNIX :

- Dans un environnement de shell C UNIX, saisissez :

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

Dans un environnement de shell Bourne UNIX, saisissez :

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

Configuration d'INFA_DEFAULT_DOMAIN sous Windows

Pour configurer INFA_DEFAULT_DOMAIN sous Windows :

- Entrez la variable d'environnement INFA_DEFAULT_DOMAIN et définissez la valeur du nom du domaine.

Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

INFA_DEFAULT_DOMAIN_PASSWORD

La variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD s'applique au programme de ligne de commande infacmd.

La plupart des commandes *infacmd* exigent un mot de passe utilisateur. Vous pouvez indiquer un mot de passe utilisateur dans l'option de la commande *infacmd* ou vous pouvez le stocker dans la variable d'environnement `INFA_DEFAULT_DOMAIN_PASSWORD`.

Suivez la procédure suivante pour utiliser un mot de passe crypté comme variable d'environnement :

1. Utilisez le programme de ligne de commande *pmpasswd* pour crypter le mot de passe utilisateur.
pmpasswd génère et affiche le mot de passe crypté. Par exemple, si vous entrez le mot de passe « lundi », il sera crypté et deviendra `f/wRb5PZsZnqESTDPeos7Q==`.
2. Configurez la variable d'environnement de mot de passe pour définir la valeur cryptée.

LIENS CONNEXES :

- [“Chiffrement des mots de passe” à la page 61](#)

Configuration d'INFA_DEFAULT_DOMAIN_PASSWORD sous UNIX

Pour configurer `INFA_DEFAULT_DOMAIN_PASSWORD` sous UNIX :

1. À la ligne de commande, saisissez :

```
pmpasswd <password>
```

pmpasswd renvoie le mot de passe crypté.
2. Dans un environnement de shell C UNIX, saisissez :

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


Dans un environnement de shell Bourne UNIX, saisissez :

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

Configuration d'INFA_DEFAULT_DOMAIN_PASSWORD sous Windows

Pour configurer `INFA_DEFAULT_DOMAIN_PASSWORD` sous Windows :

1. À la ligne de commande, saisissez :

```
pmpasswd <password>
```

pmpasswd renvoie le mot de passe crypté.
2. Entrez la variable d'environnement `INFA_DEFAULT_DOMAIN_PASSWORD` et définissez la valeur du mot de passe *crypté*.

Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

INFA_DEFAULT_DOMAIN_USER

La variable d'environnement `INFA_DEFAULT_DOMAIN_USER` s'applique au programme de ligne de commande *infacmd*.

La plupart des commandes *infacmd* exigent un nom d'utilisateur. Vous pouvez indiquer un nom d'utilisateur dans l'option de la commande *infacmd* ou vous pouvez le stocker dans la variable d'environnement `INFA_DEFAULT_DOMAIN_USER`.

Configuration d'INFA_DEFAULT_DOMAIN_USER sous UNIX

Pour configurer INFA_DEFAULT_DOMAIN_USER sous UNIX :

- Dans un environnement de shell C UNIX, saisissez :

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

Dans un environnement de shell Bourne UNIX, saisissez :

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

Configuration d'INFA_DEFAULT_DOMAIN_USER sous Windows

Pour configurer INFA_DEFAULT_DOMAIN_USER sous Windows :

- Entrez la variable d'environnement INFA_DEFAULT_DOMAIN_USER et définissez la valeur sur le nom d'utilisateur par défaut.

Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

INFA_DEFAULT_PWX_OSEPASSWORD

La variable d'environnement INFA_DEFAULT_PWX_OSEPASSWORD s'applique au programme de ligne de commande infacmd pwx.

Certaines commandes infacmd pwx exigent un mot de passe du système d'exploitation. Vous pouvez indiquer un mot de passe crypté dans l'option de la commande infacmd pwx ou vous pouvez le stocker dans la variable d'environnement INFA_DEFAULT_PWX_OSEPASSWORD.

Suivez la procédure suivante pour utiliser un mot de passe crypté comme variable d'environnement :

1. Pour crypter le mot de passe, utilisez le programme de ligne de commande pmpasswd.
Le programme pmpasswd génère et affiche le mot de passe crypté. Par exemple, si vous entrez le mot de passe « lundi », il sera crypté et deviendra f/wRb5PZsZnqESTDPeos7Q==.
2. Configurez la variable d'environnement de mot de passe pour définir la valeur cryptée.

LIENS CONNEXES :

- [“Chiffrement des mots de passe” à la page 61](#)

Configuration d'INFA_DEFAULT_PWX_OSEPASSWORD sous UNIX

Pour configurer INFA_DEFAULT_PWX_OSEPASSWORD sous UNIX :

1. À la ligne de commande, saisissez :

```
pmpasswd password
```

Le programme pmpasswd renvoie le mot de passe crypté.

2. Dans un environnement de shell C UNIX, saisissez :

```
setenv INFA_DEFAULT_PWX_OSEPASSWORD encrypted_password
```

Dans un environnement de shell Bourne UNIX, saisissez :

```
INFA_DEFAULT_PWX_OSEPASSWORD = encrypted_password  
export INFA_DEFAULT_PWX_OSEPASSWORD
```


Configuration d'INFA_DEFAULT_PWX_OSEPASSWORD sous Windows

Pour configurer INFA_DEFAULT_PWX_OSEPASSWORD sous Windows :

1. À la ligne de commande, saisissez :

```
mpasswd password
```

Le programme `mpasswd` renvoie le mot de passe crypté.

2. Entrez la variable d'environnement INFA_DEFAULT_PWX_OSEPASSWORD et définissez la valeur du mot de passe crypté.

Pour plus d'informations sur le paramétrage des variables d'environnement sous Windows, consultez la documentation Windows.

INFA_DEFAULT_PWX_OSPASSWORD

La variable d'environnement INFA_DEFAULT_PWX_OSPASSWORD s'applique au programme de ligne de commande `infacmd pwx`.

Certaines commandes `infacmd pwx` exigent un mot de passe du système d'exploitation. Vous pouvez fournir un mot de passe en texte clair dans une option de la commande `infacmd pwx` ou vous pouvez le stocker dans la variable d'environnement INFA_DEFAULT_PWX_OSPASSWORD.

Configuration d'INFA_DEFAULT_PWX_OSPASSWORD sous UNIX

Pour configurer INFA_DEFAULT_PWX_OSPASSWORD sous UNIX :

- Dans un environnement de shell C UNIX, saisissez :

```
setenv INFA_DEFAULT_PWX_OSPASSWORD password
```

Dans un environnement de shell Bourne UNIX, saisissez :

```
INFA_DEFAULT_PWX_OSPASSWORD = password  
export INFA_DEFAULT_PWX_OSPASSWORD
```

Configuration d'INFA_DEFAULT_PWX_OSPASSWORD sous Windows

Pour configurer INFA_DEFAULT_PWX_OSPASSWORD sous Windows, définissez la valeur du mot de passe en texte clair.

Pour plus d'informations sur le paramétrage des variables d'environnement sous Windows, consultez la documentation Windows.

INFA_DEFAULT_SECURITY_DOMAIN

La variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN s'applique au programme de ligne de commande `infacmd`.

Les commandes `infacmd` requièrent un domaine de sécurité si vous utilisez une authentification LDAP et que vous spécifiez un utilisateur Informatica. Vous pouvez donner à la variable d'environnement

INFA_DEFAULT_SECURITY_DOMAIN le nom du domaine de sécurité natif ou un nom de domaine de sécurité LDAP.

Configuration d'INFA_DEFAULT_SECURITY_DOMAIN sous UNIX

Pour configurer INFA_DEFAULT_SECURITY_DOMAIN sous UNIX :

- Dans un environnement de shell C UNIX, saisissez :

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

Dans un environnement de shell Bourne UNIX, saisissez :

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

Configuration d'INFA_DEFAULT_SECURITY_DOMAIN sous Windows

Pour configurer INFA_DEFAULT_SECURITY_DOMAIN sous Windows :

- Entrez la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN et définissez la valeur du nom de domaine de sécurité.

Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

INFA_DOMAINS_FILE

La variable d'environnement INFA_DOMAINS_FILE s'applique aux programmes de ligne de commande infacmd, infasetup, pmcmd et pmrep.

Lorsque vous installez les services Informatica à l'aide du programme d'installation Informatica, ce dernier crée un fichier domains.infra dans le répertoire d'installation d'Informatica. Le fichier domains.infra contient les informations de connectivité pour les nœuds de passerelle dans un domaine, dont les noms de domaines, les noms d'hôtes de domaines et les numéros de ports d'hôtes de domaines. Les programmes de ligne de commande nécessitent les informations de connectivité présentes dans le fichier domains.infra pour se connecter aux nœuds de passerelle dans un domaine. Vous pouvez définir la variable d'environnement INFA_DOMAINS_FILE sur le chemin et le nom du fichier domains.infra. Assurez-vous de configurer la variable INFA_DOMAINS_FILE sur la machine sur laquelle les services Informatica sont installés.

Configuration d'INFA_DOMAINS_FILE sous UNIX

Pour configurer INFA_DOMAINS_FILE sous UNIX :

- Dans un environnement de shell C UNIX, saisissez :

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

Dans un environnement de shell Bourne UNIX, saisissez :

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

Configuration d'INFA_DOMAINS_FILE sous Windows

Pour configurer INFA_DOMAINS_FILE sous Windows :

- Entrez la variable d'environnement INFA_DOMAINS_FILE et définissez la valeur sur le chemin et le nom du fichier domains.infa.

Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

INFA_JAVA_CMD_OPTS

La variable d'environnement INFA_JAVA_CMD_OPTS s'applique au programme de ligne de commande infasetup.

Vous pouvez configurer la variable d'environnement INFA_JAVA_CMD_OPTS pour définir les options Java telles que les valeurs -Xmx et les propriétés système. Pour définir une propriété système, passez la valeur au format suivant :

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

Par exemple, vous souhaitez peut-être augmenter la mémoire système utilisée par la commande infasetup. La mémoire système par défaut pour infasetup est 512 Mo. Pour configurer une mémoire de 1024 Mo dans un environnement C shell UNIX, entrez :

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

Configuration d'INFA_JAVA_CMD_OPTS sous UNIX

Pour configurer INFA_JAVA_CMD_OPTS sous UNIX :

- Dans un environnement de shell C UNIX, saisissez :

```
setenv INFA_JAVA_CMD_OPTS <Java_Options>
```

Dans un environnement de shell Bourne UNIX, saisissez :

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

Configuration d'INFA_JAVA_CMD_OPTS sous Windows

Pour configurer INFA_JAVA_CMD_OPTS sous Windows :

- Entrez la variable d'environnement INFA_JAVA_CMD_OPTS et définissez les options Java telles que les valeurs -Xmx et les propriétés système.

Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

INFA_PASSWORD

La variable d'environnement INFA_PASSWORD s'applique aux programmes de ligne de commande infacmd et infasetup.

Certaines commandes `infacmd` et `infasetup` exigent un mot de passe utilisateur. Vous pouvez indiquer un mot de passe utilisateur dans l'option de ces commandes ou vous pouvez le stocker dans la variable d'environnement `INFA_PASSWORD`.

Vous pouvez utiliser la variable d'environnement `INFA_PASSWORD` pour stocker différents types de mots de passe. Par exemple dans la commande `infasetup DefineDomain`, vous pouvez utiliser la variable pour définir le mot de passe de l'entrepôt de clés. Dans la commande `infacmd isp SetLDAPConnectivity`, vous pouvez utiliser la variable pour définir le mot de passe du justificatif LDAP. Vous devrez peut-être modifier la valeur de cette variable en fonction des commandes que vous exécutez.

Suivez la procédure suivante pour utiliser un mot de passe crypté comme variable d'environnement :

1. Utilisez le programme de ligne de commande `pmpasswd` pour crypter le mot de passe utilisateur.
`pmpasswd` génère et affiche le mot de passe crypté. Par exemple, si vous entrez le mot de passe « lundi », il sera crypté et deviendra `f/wRb5PZsZnqESTDPeos7Q==`.
2. Configurez la variable d'environnement de mot de passe pour définir la valeur cryptée.

LIENS CONNEXES :

- [“Chiffrement des mots de passe” à la page 61](#)

Configuration d'INFA_PASSWORD sous UNIX

Pour configurer `INFA_PASSWORD` sous UNIX :

1. À la ligne de commande, saisissez :

```
pmpasswd <password>
```


pmpasswd renvoie le mot de passe crypté.
2. Dans un environnement de shell C UNIX, saisissez :

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


Dans un environnement de shell Bourne UNIX, saisissez :

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

Configuration d'INFA_PASSWORD sous Windows

Pour configurer `INFA_PASSWORD` sous Windows :

1. À la ligne de commande, saisissez :

```
pmpasswd <password>
```


pmpasswd renvoie le mot de passe crypté.
2. Entrez la variable d'environnement `INFA_PASSWORD` et définissez la valeur du mot de passe *crypté*.
Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

INFA_NODE_KEYSTORE_PASSWORD

La variable d'environnement INFA_NODE_KEYSTORE_PASSWORD s'applique au programme de ligne de commande *infasetup*.

Certaines commandes *infasetup* configurent la communication sécurisée pour le domaine. Vous pouvez fournir le mot de passe du fichier entrepôt de clés Java (JKS, Java Keystore) Informatica en tant qu'option avec *infasetup* ou le stocker en tant que variable d'environnement INFA_NODE_KEYSTORE_PASSWORD.

Suivez la procédure suivante pour utiliser un mot de passe crypté comme variable d'environnement :

1. Utilisez le programme de ligne de commande *mpasswd* pour crypter le mot de passe utilisateur.
mpasswd génère et affiche le mot de passe crypté. Par exemple, si vous entrez le mot de passe « lundi », il sera crypté et deviendra f/wRb5PZsZnqESTDPeos7Q==.
2. Configurez la variable d'environnement de mot de passe pour définir la valeur cryptée.

Configuration de INFA_NODE_KEYSTORE_PASSWORD sous UNIX

Pour configurer INFA_NODE_KEYSTORE_PASSWORD sous UNIX :

1. Sur la ligne de commande, saisissez :

```
mpasswd <database password>
```

mpasswd renvoie le mot de passe crypté.
2. Dans un environnement de shell C UNIX, saisissez :

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

Dans un environnement de shell Bourne UNIX, saisissez :

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

Configuration de INFA_NODE_KEYSTORE_PASSWORD sous Windows

Pour configurer INFA_NODE_KEYSTORE_PASSWORD sous Windows :

1. Sur la ligne de commande, saisissez :

```
mpasswd <database password>
```

mpasswd renvoie le mot de passe crypté.
2. Entrez la variable d'environnement INFA_NODE_KEYSTORE_PASSWORD et définissez la valeur sur le mot de passe *crypté*.

Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

INFA_NODE_TRUSTSTORE_PASSWORD

La variable d'environnement `INFA_NODE_TRUSTSTORE_PASSWORD` s'applique au programme de ligne de commande `infasetup`.

Certaines commandes *infasetup* configurent la communication sécurisée pour le domaine. Vous pouvez fournir le mot de passe du fichier `infa_truststore.jks` en tant qu'option avec *infasetup* ou le stocker en tant que variable d'environnement `INFA_NODE_TRUSTSTORE_PASSWORD`.

Suivez la procédure suivante pour utiliser un mot de passe crypté comme variable d'environnement :

1. Utilisez le programme de ligne de commande `pmpasswd` pour crypter le mot de passe utilisateur. `pmpasswd` génère et affiche le mot de passe crypté. Par exemple, si vous entrez le mot de passe « lundi », il sera crypté et deviendra `f/wRb5PZsZnqESTDPeos7Q==`.
2. Configurez la variable d'environnement de mot de passe pour définir la valeur cryptée.

Configuration de INFA_NODE_TRUSTSTORE_PASSWORD sous UNIX

Pour configurer `INFA_NODE_TRUSTSTORE_PASSWORD` sous UNIX :

1. Sur la ligne de commande, saisissez :

```
pmpasswd <database password>
```

`pmpasswd` renvoie le mot de passe crypté.
2. Dans un environnement de shell C UNIX, saisissez :

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

Dans un environnement de shell Bourne UNIX, saisissez :

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

Configuration de INFA_NODE_TRUSTSTORE_PASSWORD sous Windows

Pour configurer `INFA_NODE_TRUSTSTORE_PASSWORD` sous Windows :

1. Sur la ligne de commande, saisissez :

```
pmpasswd <database password>
```

`pmpasswd` renvoie le mot de passe crypté.
2. Entrez la variable d'environnement `INFA_NODE_TRUSTSTORE_PASSWORD` et définissez la valeur du mot de passe crypté.

Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

INFA_REPCNX_INFO

La variable d'environnement `INFA_REPCNX_INFO` s'applique au programme de ligne de commande `pmrep`.

Lorsque vous exécutez *pmrep* en mode ligne de commande ou depuis un script, cette commande stocke les informations de connexion du référentiel dans un fichier, *pmrep.cnx*. *pmrep* utilise les informations de ce fichier pour se reconnecter au référentiel. La variable d'environnement *INFA_REPCNX_INFO* stocke le nom et le chemin d'accès du fichier de connexion du référentiel. Chaque fois que vous exécutez *pmrep connect*, la commande supprime le fichier *pmrep.cnx*. Si la commande *pmrep connect* s'exécute correctement, elle remplace le fichier *pmrep.cnx* par les informations de connexion du référentiel.

Utilisez cette variable lorsque les scripts qui sont à l'origine des commandes *pmrep* sont exécutés simultanément et se connectent à des référentiels différents. Spécifiez un fichier de connexion du référentiel différent dans chaque shell. Cela évite qu'un script écrase les informations de connexion utilisées par un autre script.

Si vous ne définissez pas cette variable d'environnement, *pmrep* stocke les informations de connexion dans *pmrep.cnx* dans le répertoire home. Si vous souhaitez définir le fichier *pmrep.cnx* à un autre emplacement, indiquez le chemin du fichier à l'aide de la variable d'environnement *INFA_REPCNX_INFO*.

Configuration d'INFA_REPCNX_INFO sous UNIX

Pour configurer *INFA_REPCNX_INFO* sous UNIX :

- Dans un environnement de shell C UNIX, saisissez :

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

Dans un environnement de shell Bourne UNIX, saisissez :

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

Configuration d'INFA_REPCNX_INFO sous Windows

Pour configurer *INFA_REPCNX_INFO* sous Windows :

- Dans un shell DOS, entrez :

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

Remarque: Si vous exécutez plusieurs scripts *pmrep*, définissez cette variable d'environnement pour le shell DOS et non pour la machine.

INFA_REPOSITORY_PASSWORD

La variable d'environnement *INFA_REPOSITORY_PASSWORD* s'applique au programme de ligne de commande *infacmd*.

Certaines commandes *infacmd* requièrent un mot de passe du référentiel PowerCenter. Vous pouvez indiquer un mot de passe utilisateur dans l'option de la commande *infacmd* ou vous pouvez le stocker dans la variable d'environnement *INFA_REPOSITORY_PASSWORD*.

Suivez la procédure suivante pour utiliser un mot de passe crypté comme variable d'environnement :

1. Utilisez le programme de ligne de commande *pmpasswd* pour crypter le mot de passe utilisateur.
pmpasswd génère et affiche le mot de passe crypté. Par exemple, si vous entrez le mot de passe « lundi », il sera crypté et deviendra *f/wRb5PZsZnqESTDPeos7Q==*.
2. Configurez la variable d'environnement de mot de passe pour définir la valeur cryptée.

LIENS CONNEXES :

- [“Chiffrement des mots de passe” à la page 61](#)

Configuration d'INFA_REPOSITORY_PASSWORD sous UNIX

Pour configurer INFA_REPOSITORY_PASSWORD sous UNIX :

1. À la ligne de commande, saisissez :

```
mpasswd <password>
```

mpasswd renvoie le mot de passe crypté.

2. Dans un environnement de shell C UNIX, saisissez :

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

Dans un environnement de shell Bourne UNIX, saisissez :

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

Configuration d'INFA_REPOSITORY_PASSWORD sous Windows

Pour configurer INFA_REPOSITORY_PASSWORD sous Windows :

1. À la ligne de commande, saisissez :

```
mpasswd <repository password>
```

mpasswd renvoie le mot de passe crypté.

2. Entrez la variable d'environnement INFA_REPOSITORY_PASSWORD et définissez la valeur du mot de passe crypté.

Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

INFATool_DATEFORMAT

La variable d'environnement INFATool_DATEFORMAT s'applique au programme de ligne de commande *pmcmd*.

Utilisez cette variable d'environnement pour personnaliser la manière dont *pmcmd* affiche la date et l'heure. Entrez la chaîne de format de date dans le format DY MON DD HH24:MI:SS YYYY. *pmcmd* vérifie que la chaîne est dans un format valide. Si le format de la chaîne n'est pas valide, le service d'intégration génère un message d'avertissement et affiche la date dans le format JJJ MMM JJ HH24:MI:SS AAAA.

Configuration d'INFATool_DATEFORMAT sous UNIX

Pour configurer INFATool_DATEFORMAT sous UNIX :

- Dans un environnement de shell C UNIX, saisissez :

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

Dans un environnement de shell Bourne UNIX, saisissez :

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


Configuration d'INFATool_DATEFORMAT sous Windows

Pour configurer INFATool_DATEFORMAT sous Windows :

- Entrez la variable d'environnement INFATool_DATEFORMAT et définissez la valeur du format d'affichage de la chaîne.

Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

Chiffrement des mots de passe

Vous pouvez crypter des mots de passe pour créer une variable d'environnement à utiliser avec les commandes infacmd, infasetup, pmcmd et pmrep ou pour définir un mot de passe dans un fichier de paramètres.

Par exemple, vous pouvez crypter les mots de passe du référentiel et de la base de données pour pmrep pour maintenir la sécurité lors de l'utilisation de pmrep dans les scripts. Vous pouvez créer une variable d'environnement pour stocker le mot de passe crypté. Ou vous pouvez définir un mot de passe pour un objet de connexion de la base de données relationnelle dans un fichier de paramètres.

Utilisez le programme de ligne de commande pmpasswd pour chiffrer les mots de passe.

L'utilitaire pmpasswd utilise le chiffrement de remplissage AES/CBC/PKCS5 et génère un mot de passe codé en base64 et chiffré AES 128 bits ou 256 bits.

L'utilitaire pmpasswd s'installe dans le répertoire suivant :

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

L'utilitaire pmpasswd utilise la syntaxe suivante :

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

Le tableau suivant décrit les options et arguments de pmpasswd :

Option	Argument	Description
-	Password	Obligatoire. Mot de passe à chiffrer.
-e	CRYPT_DATA, CRYPT_SYSTEM	Facultatif. Type de chiffrement : <ul style="list-style-type: none">- CRYPT_DATA. Utiliser pour crypter les mots de passe de l'objet de connexion que vous définissez dans un fichier de paramètres.- CRYPT_SYSTEM. Utiliser pour tous les autres mots de passe. La valeur par défaut est CRYPT_SYSTEM.

Par défaut, l'utilitaire pmpasswd génère un mot de passe chiffré AES 128 bits. Vous pouvez définir la variable d'environnement INFA_USE_AES_256_CRYPTOLOGRAPHER sur *True* pour activer le chiffrement AES 256 bits pour renforcer la sécurité du mot de passe. Dans un domaine à nœud unique ou à plusieurs nœuds, assurez-vous d'arrêter le domaine avant de définir ou de supprimer la variable d'environnement.

Lorsque vous activez le chiffrement AES 256 bits, les données sensibles précédemment stockées dans les variables d'environnement ne fonctionnent pas. Vous devez à nouveau chiffrer ces données sensibles précédemment stockées et réinitialiser les données dans les variables d'environnement après avoir activé le

chiffrement AES 256 bits. Cependant, les clés de licence restent chiffrées par AES 128 bits même si vous activez AES 256 bits.

Après avoir activé le chiffrement AES 256 bits pour un domaine, vous ne pouvez pas vous connecter au domaine Informatica 10.5 à partir d'une version précédente de celui-ci.

Après avoir choisi le chiffrement AES 128 bits ou 256 bits, vous devez utiliser le même mécanisme de chiffrement lorsque vous exécutez une opération de sauvegarde et de restauration ou d'exportation et d'importation. Par exemple, si vous sauvegardez un domaine ou un référentiel à l'aide du mécanisme AES 128 bits, vous devez restaurer ce domaine ou ce référentiel à l'aide du même mécanisme de chiffrement 128 bits. La restauration de domaine échoue si le chiffrement AES 256 bits est activé pour la sauvegarde d'un domaine, mais ne l'est pas lors de la restauration de ce domaine. Dans ce cas, nettoyez la base de données, activez le chiffrement 256 bits, puis restaurez le domaine.

De même, si vous exportez un domaine ou un référentiel à l'aide du mécanisme AES 128 bits, vous devez importer ce domaine ou ce référentiel à l'aide du même mécanisme de chiffrement 128 bits.

Utilisation d'un Mot de Passe en tant que variable d'environnement

Suivez la procédure suivante pour utiliser un mot de passe crypté comme variable d'environnement :

1. Utilisez le programme de ligne de commande *mpasswd* pour crypter le mot de passe.
mpasswd génère et affiche le mot de passe crypté. Par exemple, si vous entrez le mot de passe « lundi », il sera crypté et deviendra f/wRb5PZsZnqESTDPeos7Q==.
2. Configurez la variable d'environnement de mot de passe pour définir la valeur cryptée.

Configuration d'un mot de passe comme variable d'environnement sous UNIX

Pour configurer un mot de passe comme variable d'environnement sous UNIX :

1. À la ligne de commande, saisissez :

```
mpasswd <password>
```


mpasswd renvoie le mot de passe crypté.
2. Dans un environnement de shell C UNIX, saisissez :

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


Dans un environnement de shell Bourne UNIX, saisissez :

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

```
export <Password_Environment_Variable>
```


Vous pouvez affecter tout nom UNIX valide à la variable d'environnement.

Configuration d'un mot de passe comme variable d'environnement sous Windows

Pour configurer un mot de passe comme variable d'environnement sous Windows :

1. À la ligne de commande, saisissez :

```
mpasswd <password>
```


mpasswd renvoie le mot de passe crypté.
2. Entrez la variable d'environnement de mot de passe dans le champ VARIABLE. Entrez le mot de passe crypté dans le champ VALUE.

Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

Définition du nom d'utilisateur

Pour *pmcmd* et *pmrep*, vous pouvez créer une variable d'environnement pour stocker le nom d'utilisateur.

Configuration d'un Nom d'Utilisateur en tant que variable d'environnement sous UNIX

Pour configurer un nom d'utilisateur en tant que variable d'environnement sous UNIX :

- Dans un environnement de shell C UNIX, saisissez :

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

Dans un environnement de shell Bourne UNIX, saisissez :

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

Vous pouvez affecter tout nom UNIX valide à la variable d'environnement.

Configuration d'un Nom d'Utilisateur en tant que variable d'environnement sous Windows

Pour configurer un nom d'utilisateur en tant que variable d'environnement sous Windows :

- Entrez la variable d'environnement de nom d'utilisateur dans le champ Variable. Entrez le nom d'utilisateur dans le champ Value.

Pour plus d'informations sur la configuration de variables d'environnement sous Windows, consultez la documentation de Windows.

CHAPITRE 5

Utilisation d'infacmd

Ce chapitre comprend les rubriques suivantes :

- [Utilisation d'infacmd, présentation, 64](#)
- [infacmd ListPlugins, 65](#)
- [Exécution de commandes, 65](#)
- [Connexion au domaine, 66](#)
- [Codes de retour infacmd, 67](#)

Utilisation d'infacmd, présentation

infacmd est un programme de ligne de commande qui vous permet de gérer des domaines, des utilisateurs et des services. Utilisez *infacmd* pour gérer les objets et services suivants :

- **Services et processus d'applications.** Créer, activer, désactiver, supprimer et obtenir le statut des services d'applications et des processus de services associés. Services Ping. Répertoire les services et les nœuds qui les exécutent. Mettre à jour des processus du service et des options du processus de service. Vous ne pouvez pas utiliser *infacmd* pour créer les services d'une version précédente.
- **Passerelle de domaine.** Mettre à jour les informations de connectivité du nœud de passerelle.
- **Domaines.** Lier des domaines et supprimer des liens de domaines. Modifier le mot de passe de l'administrateur du domaine. Mettre à jour les options du domaine. Ajouter et supprimer les niveaux de service.
- **Dossiers.** Créer, déplacer, répertoire, mettre à jour et supprimer des dossiers. Déplacer des objets entre des dossiers.
- **Grilles.** Créer et supprimer des grilles. Répertoire des nœuds dans une grille.
- **Licences.** Ajouter, supprimer, attribuer, annuler l'attribution et répertoire des licences. Afficher les informations de licence.
- **Événements du journal.** Obtenir et purger les événements du journal. Obtenir des journaux de session et de flux de travail. Convertir des fichiers journaux à partir du format binaire au format texte.
- **Nœuds.** Mettre à jour, effectuer un ping, fermer et supprimer des nœuds. Répertoire des noms et des options de nœud. Mettre à jour le rôle de nœud. Ajouter, activer, répertoire, désactiver et supprimer des ressources de nœud. Changer un nœud d'un nœud de passerelle à un nœud de travail ou d'un nœud de travail à un nœud de passerelle. Calculer le profil du processeur pour un nœud.
- **Utilisateurs.** Créer et supprimer des utilisateurs. Réinitialiser des mots de passe utilisateur. Abonner et désabonner des utilisateurs aux alertes. Assigner des autorisations aux utilisateurs sur des objets. Activer le verrouillage du compte d'utilisateur et déverrouillez des comptes d'utilisateur.

infacmd ListPlugins

Chaque programme infacmd dispose d'un identifiant de plug-in. Lorsque vous exécutez le programme, vous incluez l'identifiant de plug-in dans le nom de programme.

Par exemple, dis est l'ID de plug-in pour le programme infacmd des services d'intégration de données.

Par exemple, pour exécuter une commande qui répertorie les applications déployées, exécutez la commande infacmd dis ListApplications :

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

Pour répertorier les ID de plug-in, entrez la commande suivante :

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

Pour répertorier les commandes valides pour un plug-in, entrez la commande suivante :

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

Pour afficher l'aide pour une commande, entrez la commande suivante :

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

Exécution de commandes

Invoquer infacmd depuis la ligne de commande. Vous pouvez exécuter les commandes directement ou à partir d'un script, un fichier de lots ou d'autres programme.

Pour exécuter des commandes infacmd :

1. À l'invite de commande, passez au répertoire abritant l'exécutable infacmd.

Par défaut, la commande infacmd s'installe dans le répertoire suivant de l'installation des services Informatica : <Informatica installation directory>/isp/bin

Vous pouvez également installer infacmd depuis le DVD d'installation d'Informatica.

2. Saisissez infacmd sous Windows ou infacmd.sh sous UNIX suivi de l'ID de plug-in, du nom de commande et des options et arguments requis. Les noms de commandes ne sont pas sensibles à la casse.

Par exemple :

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

Lorsque vous exécutez la commande infacmd, vous saisissez des options pour chaque commande, suivies par les arguments Requis. Par exemple, la plupart des commandes exigent que vous saississiez le nom de domaine, le nom d'utilisateur et le mot de passe en utilisant les options de commande. Les options de commande sont précédées par un trait d'union et ne sont pas sensibles à la casse. Les arguments suivent l'option.

Pour entrer un argument précédé par un trait d'union, placez l'argument entre guillemets à l'aide de la barre oblique inversée (\) comme caractère d'échappement avant chaque guillemet. Par exemple, la commande suivante écrit le journal de l'exécution du mappage dont l'ID de tâche est « -qnLI7G_TEeW9oIHBkc9hoA » dans le fichier « MyLog.log » du répertoire infacmd sous Windows :

```
infacmd ms GetRequestLog -dn MyDomain -sn MyDIS -un AdminUser -pd password -id \"-  
qnLI7G_TEeW9oIHBkc9hoA\" -f MyLog.log
```

Si vous omettez ou entrez de manière incorrecte l'une des options requises, la commande échoue et infacmd renvoie un message d'erreur.

Vous pouvez utiliser les variables d'environnement pour certaines options de commande avec la commande infacmd. Par exemple, vous pouvez stocker le nom d'utilisateur et le mot de passe par défaut d'un domaine comme variables d'environnement, de sorte que vous n'aurez pas à les entrer en utilisant les options de commande. Configurez ces variables avant d'utiliser infacmd.

Connexion au domaine

Le programme de ligne de commande infacmd contient des options que vous utilisez pour vous connecter au domaine. Ces options sont communes pour toutes les commandes.

Le tableau suivant décrit les options infacmd communes à toutes les commandes :

Option	Description
-DomainName -dn	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Obligatoire si le domaine utilise l'authentification native ou LDAP. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique. Si le domaine utilise un domaine Kerberos unique pour l'authentification, spécifiez l'élément samAccountName pour l'utilisateur. Si le domaine utilise l'authentification inter-domaines Kerberos, spécifiez le nom du principal de l'utilisateur.
-Password -pd	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Description
-SecurityDomain -sdn	<p>Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Vous pouvez spécifier une valeur pour -sdn ou utiliser la valeur par défaut selon le mode d'authentification :</p> <ul style="list-style-type: none"> - Requis si le domaine utilise l'authentification LDAP. Pour travailler avec l'authentification LDAP, vous devez spécifier la valeur pour -sdn. - Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Si le domaine utilise l'authentification native, la valeur par défaut est native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation. <p>La valeur par défaut est Natif.</p>
-ResilienceTimeout -re	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>

Codes de retour infacmd

Le programme infacmd indique la réussite ou l'échec d'une commande à l'aide des codes de retour suivants :

- 0 indique que la commande a réussi.
- -1 indique que la commande a échoué.

Utilisez la commande DOS ou UNIX « echo » immédiatement après avoir exécuté une commande infacmd pour voir le code de retour de cette commande :

- Dans un shell DOS : `echo %ERRORLEVEL%`
- Dans un shell UNIX Bourne ou Korn : `echo $?`
- Dans un shell C UNIX : `echo $status`

CHAPITRE 6

infacmd comme Référence de commande

Ce chapitre comprend les rubriques suivantes :

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

CreateExceptionAuditTables

Crée des table pouvant contenir les données de suivi d'audit du travail effectué par les utilisateurs de l'outil Analyst tool dans des tâches de gestion des exceptions.

La commande infacmd CreateExceptionAuditTables utilise la syntaxe suivante :

```
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]
```

Remarque: Le programme infacmd utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit les options de la commande `infacmd as CreateExceptionAuditTables` :

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-ServiceName -sn	Requis. Nom du service Analyst.
-UserName -un	Nom d'utilisateur pour se connecter au domaine.
-Password -pd	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-ResilienceTimeout -re	Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine.

Règles et directives pour les tables d'audit de gestion des exceptions

Avant de créer des tables pour stocker les données d'audit des tâches de gestion des exceptions, consultez les règles et directives suivantes :

- Le service Analyst écrit les données d'audit des tâches de gestion des exceptions créées par un service d'intégration de données lors de l'exécution d'un flux de travail contenant une tâche humaine. Chaque tâche de gestion des exceptions est une instance d'une tâche humaine dans un flux de travail.

L'option `HumanTaskDataIntegrationService` dans la commande d'aide `infacmd createService` identifie le service d'intégration de données qui crée les tâches de gestion des exceptions.

- Avant de créer les tables de gestion des exceptions, identifiez une base de données et un schéma pour celles-ci. Pour identifier la base de données et le schéma, exécutez la commande `infacmd updateServiceOptions`.

Lorsque vous exécutez la commande `infacmd updateServiceOptions`, définissez les options suivantes :

- o `HumanTaskDataIntegrationService.exceptionDbName`
- o `HumanTaskDataIntegrationService.exceptionSchemaName`

- Les tables d'audit contiennent toutes les données de suivi d'audit du travail effectué par les utilisateurs de l'outil Analyst tool que le service Analyst spécifie. Si vous ne créez pas les tables d'audit, le service Analyst crée des tables d'audit pour chaque tâche de gestion des exceptions dans la base de données qui contient les données des tâches.

CreateService

Crée un service Analyst dans un domaine. Associe également un service de référentiel modèle, des services d'intégration de données et un service Metadata Manager au service Analyst.

La commande infacmd as CreateService utilise la syntaxe suivante :

```
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
```

Remarque: Le programme infacmd utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit les options de la commande infacmd as CreateService :

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-NodeName -nn	Requis. Nom du nœud sur lequel le service Analyst s'exécutera.
-ServiceName -sn	Requis. Nom du service Analyst. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 230 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "
-UserName -un	Nom d'utilisateur pour se connecter au domaine.
-Password -pd	Mot de passe pour le nom d'utilisateur.

Option	Description
-SecurityDomain -sdn	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-ResilienceTimeout -re	Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine.
-RepositoryService -rs	Facultatif. Nom du service de référentiel modèle. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 230 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "
-DataIntegrationService -ds	Facultatif. Nom du service d'intégration de données associé au service Analyst.
-HumanTaskDataIntegrationService -htds	Facultatif. Service d'intégration de données qui exécute des flux de travail. Lorsqu'un flux de travail contient une tâche humaine, les utilisateurs se connectent à l'URL du service Analyst pour travailler sur les instances de tâche humaine.
-MetadataManagerService -mm	Facultatif. Nom du service Metadata Manager associé au service Analyst.
-FlatFileCacheLocation -ffl	Facultatif. Chemin d'accès complet, sans le nom de domaine, du dossier dans lequel vous souhaitez mettre en cache les fichiers plats. Doit être au format suivant : /<parent folder>/>child folder>
-CatalogService -cs	Facultatif. Nom du service de catalogue que vous souhaitez associer au service Analyst.
-CatalogServiceUserName -csau	Facultatif. Requis si vous spécifiez le service de catalogue. Nom d'utilisateur administrateur pour se connecter au service de catalogue.
-CatalogServiceSecurityDomain -cssdn	Requis si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'administrateur.
-CatalogServicePassword -csap	Requis si vous spécifiez un service de catalogue. Mot de passe de l'utilisateur du service de catalogue.
-RepositoryUserName -au	Requis si vous spécifiez un service de référentiel modèle. Nom d'utilisateur pour la connexion au référentiel modèle. Si vous entrez un nom d'utilisateur qui contient un espace ou tout autre caractère non alphanumérique, placez-le entre guillemets.
-RepositorySecurityDomain -rssdn	Requis si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'administrateur.
-RepositoryPassword -ap	Requis si vous spécifiez un service de référentiel modèle. Mot de passe utilisateur pour le service de référentiel modèle.

Option	Description
-BusinessGlossaryExportFileDirectory -bgefd	Facultatif. Emplacement du répertoire d'exportation des fichiers de glossaire métier.
-HttpPort	Requis. Numéro de port pour le service Analyst.

DeleteExceptionAuditTables

Supprime des tables pouvant contenir les données de suivi d'audit du travail effectué par les utilisateurs de l'outil Analyst tool dans des tâches de gestion des exceptions.

La commande infacmd as DeleteExceptionAuditTables utilise la syntaxe suivante :

```
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]
```

Remarque: Le programme infacmd utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit les options de la commande infacmd as DeleteExceptionAuditTables :

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-ServiceName -sn	Requis. Nom du service Analyst.
-UserName -un	Nom d'utilisateur pour se connecter au domaine.
-Password -pd	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-ResilienceTimeout -re	Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine.

ListServiceOptions

Répertorie les options de service Analyst. Répertorie les valeurs pour chaque option de service Analyst.

La commande infacmd as ListServiceOptions utilise la syntaxe suivante :

```
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]
```

Remarque: Le programme infacmd utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit la commande infacmd as ListServiceOptions :

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-ServiceName -sn	Requis. Nom du service Analyst. Le nom n'est pas sensible à la casse.
-UserName -un	Nom d'utilisateur pour se connecter au domaine.
-Password -pd	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-ResilienceTimeout -re	Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine.

ListServiceProcessOptions

Répertorie les options du processus du service Analyst.

La commande infacmd as ListServiceProcessOptions utilise la syntaxe suivante :

```
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
```

Remarque: Le programme infacmd utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit la commande infacmd as ListServiceProcessOptions :

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-ServiceName -sn	Requis. Nom du service Analyst. Le nom n'est pas sensible à la casse.
-UserName -un	Nom d'utilisateur pour se connecter au domaine.
-Password -pd	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-ResilienceTimeout -re	Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine.
-NodeName -nn	Obligatoire. Nœud sur lequel s'exécute le processus du service Analyst.

UpdateServiceOptions

Met à jour les options du service Analyst. Pour afficher les valeurs des options actuelles, exécutez la commande as ListServiceOptions.

La commande infacmd as UpdateServiceOptions utilise la syntaxe suivante :

```
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]
```

Remarque: Le programme infacmd utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit la commande infacmd as UpdateServiceOptions :

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-ServiceName -sn	Requis. Nom du service Analyst. Le nom n'est pas sensible à la casse.
-UserName -un	Nom d'utilisateur pour se connecter au domaine.
-Password -pd	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-ResilienceTimeout -re	Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine.
-Options -o	Facultatif. Liste des options à configurer. Séparez chaque option par un espace. Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets. Par exemple : ... -o option_name=value option_name="value 2" ... Pour afficher des options, exécutez la commande infacmd as ListServiceOptions.

UpdateServiceProcessOptions

Met à jour les options du processus de service Analyst. Pour afficher les options, exécutez la commande infacmd as ListServiceProcessOptions.

La commande infacmd as UpdateServiceProcessOptions utilise la syntaxe suivante :

```
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
```

Remarque: Le programme infacmd utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit la commande infacmd as UpdateServiceProcessOptions :

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-ServiceName -sn	Requis. Nom du service Analyst.
-UserName -un	Nom d'utilisateur pour se connecter au domaine.
-Password -pd	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-ResilienceTimeout -re	Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine.
-NodeName -nn	Obligatoire. Nœud sur lequel s'exécute le processus du service Analyst.
-Options -o	Obligatoire. Liste des options à configurer. Séparez chaque option par un espace. Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets. Par exemple : ... -o option_name=value option_name="value 2" ... Pour afficher les options, exécutez la commande infacmd as ListServiceProcessOptions.

CHAPITRE 7

infacmd aud Command Reference

Ce chapitre comprend les rubriques suivantes :

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

getDomainObjectPermissions

Obtient la liste des objets de domaine pour lesquels les utilisateurs ou groupes spécifiés possèdent une autorisation. Vous pouvez générer des rapports pour les utilisateurs ou groupe spécifiés.

Les utilisateurs possédant le rôle Administrateur peuvent exécuter cette commande.

La commande infacmd aud getDomainObjectPermissions utilise la syntaxe suivante :

```
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]
```

Remarque: Le programme infacmd utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit les options et arguments d'infacmd aud getDomainObjectPermissions :

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-UserName -un	Nom d'utilisateur pour se connecter au domaine.
-Password -pd	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	Nom du domaine de sécurité que vous voulez créer et auquel l'utilisateur du domaine appartient.
-Gateway -hp	Obligatoire si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Spécifiez les noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine.
-ExistingUserNames -eu	Obligatoire si vous n'utilisez pas -ExistingGroupNames (-eg). Nom de l'utilisateur ou liste d'utilisateurs pour exécuter les rapports. Pour plusieurs utilisateurs, séparez chaque utilisateur par une virgule dans la ligne de commande.
-ExistingGroupNames -eg	Obligatoire si vous n'utilisez pas -ExistingUserName (-eu). Nom du groupe ou liste de groupes pour exécuter les rapports. Pour plusieurs groupes, séparez chaque groupe par une virgule dans la ligne de commande.
-ExistingSecurityDomain -esd	Obligatoire si vous utilisez l'authentification LDAP. Domaine de sécurité auquel l'utilisateur ou le groupe appartient. La valeur par défaut est Native.
-Format -fm	Facultatif. Format de fichier de sortie. Les types valides comprennent : - Texte - CSV Si vous ne spécifiez aucun format, infacmd utilise le format texte avec des lignes limitées à 80 caractères.
-OutputFile -lo	Facultatif. Nom et chemin du fichier pour le fichier de sortie. Si vous ne spécifiez pas un nom de fichier de sortie, infacmd affiche les événements du journal sur l'écran.

getPrivilegeAssociation

Obtient les privilèges affectés aux utilisateurs ou groupes. Vous pouvez sélectionner les utilisateurs ou les groupes pour lesquels vous voulez générer le rapport.

Les utilisateurs possédant le rôle Administrateur peuvent exécuter cette commande.

La commande infacmd aud getPrivilegeAssociation utilise la syntaxe suivante :

```
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]
```

Remarque: Le programme infacmd utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit les options et arguments d'infacmd aud getPrivilegeAssociation :

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-UserName -un	Nom d'utilisateur pour se connecter au domaine.
-Password -pd	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine.
-ExistingUserNames -eu	Obligatoire si vous n'utilisez pas -ExistingGroupNames (-eg). Nom de l'utilisateur ou liste d'utilisateurs pour exécuter les rapports. Pour plusieurs utilisateurs, séparez chaque utilisateur par une virgule dans la ligne de commande.
-ExistingGroupNames -eg	Obligatoire si vous n'utilisez pas -ExistingUserName (-eu). Nom du groupe ou liste de groupes pour exécuter les rapports. Pour plusieurs groupes, séparez chaque groupe par une virgule dans la ligne de commande.
-ExistingSecurityDomain -esd	Obligatoire si vous utilisez l'authentification LDAP. Domaine de sécurité auquel l'utilisateur ou le groupe appartient. La valeur par défaut est Native.

Option	Description
-Format -fm	Facultatif. Format de fichier de sortie. Les types valides comprennent : - Texte - CSV Si vous ne spécifiez aucun format, infacmd utilise le format texte avec des lignes limitées à 80 caractères.
-OutputFile -lo	Facultatif. Nom et chemin du fichier pour le fichier de sortie. Si vous ne spécifiez pas un nom de fichier de sortie, infacmd affiche les événements du journal sur l'écran.

getUserGroupAssociation

Obtient la liste des utilisateurs qui appartiennent au groupe ou à une liste de groupes associés aux utilisateurs spécifiés. Vous pouvez sélectionner les utilisateurs ou les groupes pour lesquels vous voulez générer le rapport.

Les utilisateurs possédant le rôle Administrateur peuvent exécuter cette commande.

La commande infacmd aud getUserGroupAssociation utilise la syntaxe suivante :

```
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]
```

Remarque: Le programme infacmd utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit les options et arguments d'infacmd aud getUserGroupAssociation :

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-UserName -un	Nom d'utilisateur pour se connecter au domaine.
-Password -pd	Mot de passe pour le nom d'utilisateur.

Option	Description
-SecurityDomain -sdn	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine.
-ExistingUserNames -eu	Obligatoire si vous n'utilisez pas -ExistingGroupNames (-eg). Nom de l'utilisateur ou liste d'utilisateurs pour exécuter les rapports. Pour plusieurs utilisateurs, séparez chaque utilisateur par une virgule dans la ligne de commande.
-ExistingGroupNames -eg	Obligatoire si vous n'utilisez pas -ExistingUserName (-eu). Nom du groupe ou liste de groupes pour exécuter les rapports. Pour plusieurs groupes, séparez chaque groupe par une virgule dans la ligne de commande.
-ExistingSecurityDomain -esd	Obligatoire si vous utilisez l'authentification LDAP. Domaine de sécurité auquel l'utilisateur ou le groupe appartient. La valeur par défaut est Native.
-Format -fm	Facultatif. Format de fichier de sortie. Les types valides comprennent : - Texte - CSV Si vous ne spécifiez aucun format, infacmd utilise le format texte avec des lignes limitées à 80 caractères.
-OutputFile -lo	Facultatif. Nom et chemin du fichier pour le fichier de sortie. Si vous ne spécifiez pas un nom de fichier de sortie, infacmd affiche les événements du journal sur l'écran.

getUserGroupAssociationForRoles

Obtient la liste des rôles assignés aux utilisateurs et aux groupes. Vous pouvez sélectionner les rôles pour lesquels vous voulez générer le rapport.

Les utilisateurs possédant le rôle Administrateur peuvent exécuter cette commande.

La commande infacmd aud getUserGroupAssociationForRoles utilise la syntaxe suivante :

```
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]
```

Remarque: Le programme infacmd utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau

d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit les options et arguments d'infacmd aud `getUserGroupAssociationForRoles` :

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-UserName -un	Nom d'utilisateur pour se connecter au domaine.
-Password -pd	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	Requis si les informations de connectivité de passerelle du fichier <code>domains.inf</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine.
-RoleNames -en	Obligatoire. Nom du rôle attribué aux utilisateurs ou aux groupes dans le domaine pour lequel vous voulez générer le rapport. Pour plusieurs rôles, séparez chaque rôle par une virgule dans la ligne de commande.
-Format -fm	Facultatif. Format de fichier de sortie. Les types valides comprennent : - Texte - CSV Si vous ne spécifiez aucun format, infacmd utilise le format texte avec des lignes limitées à 80 caractères.
-OutputFile -lo	Facultatif. Nom et chemin du fichier pour le fichier de sortie. Si vous ne spécifiez pas un nom de fichier de sortie, infacmd affiche les événements du journal sur l'écran.

getUsersPersonalInfo

Obtient les informations utilisateur dans le domaine. Le rapport affiche le nom complet, le domaine de sécurité, la description, les détails du contact et l'état de l'utilisateur. Si vous exécutez le rapport pour des utilisateurs, le rapport affiche les informations utilisateur pour les utilisateurs spécifiés. Si vous exécutez le rapport pour des groupes, le rapport organise les informations utilisateur pour tous les utilisateurs du groupe spécifié. Le rapport affiche les groupes imbriqués séparément.

Les utilisateurs possédant le rôle Administrateur peuvent exécuter cette commande.

La commande infacmd aud `getUsersPersonalInfo` utilise la syntaxe suivante :

```
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]

```

Remarque: Le programme infacmd utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit les options et arguments d' infacmd aud getUsersPersonalInfo:

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-UserName -un	Nom d'utilisateur pour se connecter au domaine.
-Password -pd	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine
-ExistingUserNames -eu	Obligatoire si vous n'utilisez pas -ExistingGroupNames (-eg). Nom de l'utilisateur ou liste d'utilisateurs pour exécuter les rapports. Pour plusieurs utilisateurs, séparez chaque utilisateur par une virgule dans la ligne de commande.
-ExistingGroupNames -eg	Obligatoire si vous n'utilisez pas -ExistingUserName (-eu). Nom du groupe ou liste de groupes pour exécuter les rapports. Pour plusieurs groupes, séparez chaque groupe par une virgule dans la ligne de commande.
-ExistingSecurityDomain -esd	Obligatoire si vous utilisez l'authentification LDAP. Domaine de sécurité auquel l'utilisateur ou le groupe appartient. La valeur par défaut est Native.

Option	Description
-Format -fm	Facultatif. Format de fichier de sortie. Les types valides comprennent : - Texte - CSV Si vous ne spécifiez aucun format, infacmd utilise le format texte avec des lignes limitées à 80 caractères.
-OutputFile -lo	Facultatif. Nom et chemin du fichier pour le fichier de sortie. Si vous ne spécifiez pas un nom de fichier de sortie, infacmd affiche les événements du journal sur l'écran.

CHAPITRE 8

Référence de commande infacmd autotune

- [Autotune, 85](#)

Autotune

Configure les services et connexions avec les paramètres recommandés en fonction du type de déploiement. Les modifications sont appliquées après redémarrage des services.

Pour chaque service spécifié, les modifications du service sont appliquées sur tous les nœuds actuellement configurés pour exécuter le service. Les modifications affectent ainsi tous les processus de service.

La syntaxe de la commande infacmd autotune Autotune est la suivante :

```
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]
```

Le programme infacmd utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher plus d'informations sur la connexion au domaine, consultez la Référence de commande.

Le tableau suivant décrit les options et arguments de d'infacmd autotune Autotune :

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-UserName -un	Nom d'utilisateur pour se connecter au domaine.

Option	Description
-Password -pd	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-ResilienceTimeout -re	Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine.
-Size -s	Obligatoire. Type de déploiement qui représente la configuration requise du traitement de Big Data en fonction de l'accès concurrentiel et du volume. Vous pouvez entrer Sandbox, Basique, Standard ou Avancé.
-ServiceNames -sn	Facultatif. Liste des services configurés dans le domaine Informatica. Séparez chaque nom de service par une virgule. Vous pouvez régler les services suivants : <ul style="list-style-type: none"> - Service Analyst - Service de gestion de contenu - Service d'intégration de données - Service de référentiel modèle - Service de gestionnaire de ressource - Service de recherche La valeur par défaut est Aucun.
-BlazeConnectionNames -bcn	Facultatif. Liste des connexions Hadoop configurées dans le domaine Informatica. Pour chaque connexion Hadoop, la commande règle les propriétés de configuration de Blaze dans la connexion Hadoop. Séparez chaque nom de connexion Hadoop par une virgule. La valeur par défaut est Aucun.
-SparkConnectionNames -scn	Facultatif. Liste des connexions Hadoop configurées dans le domaine Informatica. Pour chaque connexion Hadoop, la commande règle les propriétés de configuration de Spark dans la connexion Hadoop. Séparez chaque nom de connexion Hadoop par une virgule. La valeur par défaut est Aucun.
-All -a	Facultatif. Entrez yes pour appliquer les paramètres recommandés à tous les services Analyst, services de gestion de contenu, services d'intégration de données, services de référentiel modèle, services de gestionnaire de ressources, services de recherche et connexions Hadoop dans le domaine Informatica. Entrez no pour appliquer les paramètres recommandés uniquement aux services et connexions Hadoop que vous spécifiez. La valeur par défaut est no .

CHAPITRE 9

Référence de commande infacmd bg

Ce chapitre comprend les rubriques suivantes :

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

upgradeRepository

Met à niveau les données de glossaire d'entreprise dans le référentiel modèle. Exécutez cette commande après la mise à niveau du domaine et du service de référentiel modèle.

La commande infacmd bg upgradeRepository utilise la syntaxe suivante :

```
upgradeRepository

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

Remarque: Le programme infacmd utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit les options et les arguments de la commande infacmd bg upgradeRepository :

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-UserName -un	Nom d'utilisateur pour se connecter au domaine.

Option	Description
-Password -pd	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
AtServiceName -atn	Requis. Nom du service Analyst. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 230 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "

deleteAuditHisotry

Supprime l'historique de l'audit d'un glossaire de l'outil Analyst tool.

La syntaxe de la commande infacmd bg deleteAuditHistory est la suivante :

```
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
```

Remarque: Le programme infacmd utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit les options et les arguments de la commande infacmd bg deleteAuditHistory :

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-UserName -un	Nom d'utilisateur pour se connecter au domaine.
-Password -pd	Mot de passe pour le nom d'utilisateur.

Option	Description
-SecurityDomain -sdn	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
AtServiceName -atn	Requis. Nom du service Analyst. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 230 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "
-GlossaryIdentity -gl	Obligatoire. Identité du glossaire pour lequel vous souhaitez supprimer l'historique de l'audit. Vous pouvez obtenir l'identité du glossaire dans la base de données du service de référentiel modèle à l'aide de l'option <code>select PSB_EXTERNID from PO_BGGLOSSARY where POB_NAME = '<glossary_name>'</code> .

listGlossary

Affiche une liste des glossaires d'entreprise disponibles dans l'outil Analyst tool en tant que sortie standard. Chaque nom de glossaire est affiché dans une ligne distincte.

La syntaxe de la commande `infacmd bg listGlossary` est la suivante :

```
listGlossary

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

Remarque: Le programme `infacmd` utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit les options et les arguments de la commande `infacmd bg upgradeRepository` :

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-UserName -un	Nom du domaine Informatica.
-Password -pd	Mot de passe pour le nom d'utilisateur.

Option	Description
-SecurityDomain -sdn	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
AtServiceName -atn	Requis. Nom du service Analyst. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 230 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "

exportGlossary

Exporte les glossaires d'entreprise disponibles dans l'outil Analyst tool. L'outil Analyst tool exporte les données du glossaire d'entreprise au format .xlsx ou .zip en fonction des options que vous spécifiez.

La syntaxe de la commande infacmd bg exportGlossary est la suivante :

```
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
```

Remarque: Le programme infacmd utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit les options et les arguments de la commande infacmd bg exportGlossary :

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-UserName -un	Nom d'utilisateur pour se connecter au domaine.
-Password -pd	Mot de passe pour le nom d'utilisateur.

Option	Description
-SecurityDomain -sdn	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
AtServiceName -atn	Requis. Nom du service Analyst. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 230 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "
-GlossaryList -gl	Facultatif. Noms du ou des glossaires que vous voulez exporter et auxquels vous avez accès, selon les autorisations et les privilèges définis dans l'outil Analyst tool. Séparez les noms des glossaires par le caractère délimiteur défini par l'utilisateur. Si vous ne spécifiez pas les noms des glossaires, l'outil Analyst tool exporte tous les glossaires auxquels vous êtes autorisé à accéder, selon les autorisations et les privilèges définis dans l'outil Analyst tool.
-Delimiter -dl	Facultatif. Spécifiez un délimiteur personnalisé si vous exportez plusieurs glossaires et que l'un d'eux comprend un caractère délimiteur standard dans son nom. Le délimiteur standard est la virgule. Définissez un délimiteur personnalisé d'un caractère spécial au maximum. Utilisez-le pour séparer les noms des glossaires.
-IncludeCrossGlossaryLinks -cgl	Facultatif. Entrez l'une des valeurs suivantes : - True pour inclure les liens des glossaires dans le fichier d'exportation. - False pour ignorer les liens des glossaires et ne pas les inclure dans le fichier d'exportation. La valeur par défaut est True .
-IncludeAuditHistory -ah	Facultatif. Entrez l'une des valeurs suivantes : - True pour inclure l'historique du suivi d'audit dans le fichier d'exportation. - False pour ignorer l'historique du suivi d'audit et ne pas l'inclure dans le fichier d'exportation. La valeur par défaut est False .
-IncludeAttachments -att	Facultatif. Entrez l'une des valeurs suivantes : - True pour inclure des pièces jointes dans le fichier d'exportation. - Spécifiez False pour ignorer les pièces jointes et ne pas les inclure dans le fichier d'exportation. La valeur par défaut est False .
-IncludeOnlyTemplates -tem	Facultatif. Entrez l'une des valeurs suivantes : - True pour inclure uniquement les modèles dans le fichier d'exportation. - False pour inclure les modèles et les données du glossaire dans le fichier d'exportation. La valeur par défaut est False .
-ExportasPlainTextOnly -ept	Facultatif. Entrez l'une des valeurs suivantes : - True pour exporter le contenu en texte enrichi formaté en texte brut. - False pour exporter le contenu en texte enrichi formaté en texte enrichi. La valeur par défaut est False .

Option	Description
-status -s	Facultatif. Entrez l'une des valeurs suivantes ou toutes les valeurs séparées par une virgule : <ul style="list-style-type: none"> - Actif pour exporter les ressources actives. - Inactif pour exporter les ressources inactives. Si vous ne spécifiez aucune valeur, l'outil Analyst tool exporte les ressources actives et inactives.
-phase -p	Facultatif. Entrez l'une des valeurs suivantes ou toutes les valeurs séparées par une virgule : <ul style="list-style-type: none"> - Brouillon pour exporter les ressources qui se trouvent dans la phase Brouillon. - En cours de vérification pour exporter les ressources qui se trouvent dans la phase En cours de vérification. - Publié pour exporter les ressources qui se trouvent dans la phase Publié. - Rejeté pour exporter les ressources qui se trouvent dans la phase Rejeté. - En attente de publication pour exporter les ressources qui se trouvent dans la phase En attente de publication. Si vous ne spécifiez aucune valeur, l'outil Analyst tool exporte toutes les ressources quelle que soit leur phase.
-ExportFilePath -ep	Requis. Spécifiez le chemin vers lequel le programme de ligne de commande doit stocker les fichiers exportés.

importGlossary

Importe des glossaires d'entreprise depuis des fichiers .xlsx ou .zip exportés à partir de l'outil Analyst tool.

La syntaxe de la commande infacmd bg importGlossary est la suivante :

```
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]
```

Remarque: Le programme infacmd utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit les options et les arguments de la commande `infacmd bg importGlossary` :

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-UserName -un	Nom d'utilisateur pour se connecter au domaine.
-Password -pd	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
AtServiceName -atn	Requis. Nom du service Analyst. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 230 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "
GlossaryList -gl	Facultatif. Noms du ou des glossaires que vous voulez importer et auxquels vous avez accès, selon les autorisations et les privilèges définis dans l'outil Analyst tool. Les glossaires doivent être figurés dans le fichier .xlsx. Séparez les noms des glossaires par le caractère délimiteur défini par l'utilisateur. Si vous ne spécifiez pas les noms des glossaires, l'outil Analyst tool importe tous les glossaires auxquels vous êtes autorisé à accéder, selon les autorisations et les privilèges définis dans l'outil Analyst tool.
-Delimiter -dl	Facultatif. Spécifiez un délimiteur personnalisé si vous importez plusieurs glossaires et que l'un d'eux comprend un caractère délimiteur standard dans son nom. Le délimiteur standard est la virgule. Définissez un délimiteur personnalisé d'un caractère spécial au maximum. Utilisez-le pour séparer les noms des glossaires.
IncludeCrossGlossaryLinks -cgl	Facultatif. Entrez l'une des valeurs suivantes : - <code>True</code> pour importer les liens des glossaires à partir du fichier d'exportation. - <code>False</code> pour ignorer l'importation de ces liens à partir du fichier d'exportation. La valeur par défaut est <code>True</code> .
-IncludeAuditHistory -ah	Facultatif. Entrez l'une des valeurs suivantes : - <code>True</code> pour importer l'historique du suivi d'audit à partir du fichier d'exportation. - <code>False</code> pour ignorer l'importation de l'historique à partir du fichier d'exportation. La valeur par défaut est <code>False</code> .

Option	Description
-IncludeAttachments -att	Facultatif. Entrez l'une des valeurs suivantes : <ul style="list-style-type: none"> - True pour inclure des pièces jointes lors de l'importation des glossaires d'entreprise. - False pour inclure les modèles et les données de glossaire lors de l'importation des glossaires d'entreprise. La valeur par défaut est True.
-IncludeOnlyTemplates -tem	Requis. Entrez l'une des valeurs suivantes : <ul style="list-style-type: none"> - True pour inclure uniquement les modèles lors de l'importation des glossaires d'entreprise. - False pour inclure les modèles et les données de glossaire lors de l'importation des glossaires d'entreprise. La valeur par défaut est False.
-IncludeRichTextContentforConflictingAssets -irt	Facultatif. Entrez l'une des valeurs suivantes : <ul style="list-style-type: none"> - True si vous souhaitez importer du contenu en texte enrichi pour les ressources en conflit. - False si vous ne souhaitez pas importer de contenu en texte enrichi pour les ressources en conflit. La valeur par défaut est True.
-ImportFilePath -ip	Requis. Spécifiez le chemin d'accès et le nom de fichier dans lequel le fichier d'importation est disponible.
-ResolutionOnMatchByName -rmn	Facultatif. Entrez l'une des valeurs suivantes : <ul style="list-style-type: none"> - Copier pour copier toutes les ressources lorsqu'un conflit de nom se produit. - Remplacer pour remplacer toutes les ressources lorsqu'un conflit de nom se produit. Il s'agit de la valeur par défaut. - Ignorer pour ignorer toutes les ressources lorsqu'un conflit de nom se produit.
-ResolutionOnMatchById -rmi	Facultatif. Entrez l'une des valeurs suivantes : <ul style="list-style-type: none"> - Copier pour copier toutes les ressources lorsqu'un conflit d'ID de ressource se produit. - Remplacer pour remplacer toutes les ressources lorsqu'un conflit d'ID de ressource se produit. Il s'agit de la valeur par défaut. - Ignorer pour ignorer toutes les ressources lorsqu'un conflit d'ID de ressource se produit.

CHAPITRE 10

Référence de commande infacmd ccps

Ce chapitre comprend les rubriques suivantes :

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

deleteClusters

Supprime les clusters créés par le flux de travail de cluster à partir de la plate-forme du nuage.

La syntaxe de la commande infacmd ccps deleteClusters est la suivante :

```
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]
```

Remarque: Lorsque vous utilisez cette commande pour supprimer des clusters sur la plate-forme du nuage Azure, le processus bloque toute autre commande via l'interpréteur de commandes jusqu'à ce que la plate-forme du nuage Azure termine le processus de libération des ressources du cluster. Ce processus pourrait prendre plusieurs minutes. Si vous essayez de détruire la commande en utilisant CTRL-C, puis la réexécutez, le délai et bloc identiques s'appliquent.

Le tableau suivant décrit les options et arguments d'infacmd ccps deleteClusters :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-CloudProvisioningConfigurationID -cpcid	cloud_provisioning_configuration_id	Obligatoire. ID de la configuration de provisionnement du nuage.
-ClusterIDs -cids	cluster_ids	Obligatoire. Liste séparée par des virgules de clusters à supprimer. L'ID de cluster est identique à celui répertorié sur le site de la plate-forme du nuage.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConfigurationName -cn	Nom de la configuration du cluster	Obligatoire. Nom de la configuration du cluster sur le domaine. Les valeurs ne sont pas sensibles à la casse.
-DeleteConnections -dc	delete_associated_connection	Facultatif. Supprime les connexions créées par la configuration de cluster. Utilisez l'une des valeurs suivantes : - TRUE - FALSE La valeur par défaut est False.

listClusters

Répertorie les clusters que le flux de travail de cluster crée et qui existent sur la plate-forme du nuage.

La syntaxe de la commande infacmd ccps listClusters est la suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd ccps listClusters :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-CloudProvisioningConfigurationID -cpcid	cloud_provisioning_configuration_id	Obligatoire. ID de la configuration de provisionnement du nuage.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

updateADLSCertificate

Met à jour le chemin du certificat de principal de service Azure Data Lake dans une configuration de provisionnement de nuage.

La syntaxe de la commande infacmd ccps updateADLSCertificate est la suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd ccps updateADLSCertificate :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-CloudProvisioningConfigurationID -cpcid	cloud_provisioning_configuration_id	Obligatoire. ID de la configuration de provisionnement de nuage à mettre à jour avec le chemin de fichier de certificat.
-CertificateFilePath -certPath	certificate_file_path	Obligatoire. Chemin d'accès au certificat de principal de service ADLS sur la machine exécutant le service d'intégration de données.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.</p>

CHAPITRE 11

Référence de commande de cluster infacmd

Ce chapitre comprend les rubriques suivantes :

- [createConfiguration, 101](#)
- [createConfigurationWithParams, 104](#)
- [deleteConfiguration, 106](#)
- [clearConfigurationProperties, 108](#)
- [exportConfiguration, 110](#)
- [listAssociatedConnections, 112](#)
- [listConfigurationGroupPermissions, 113](#)
- [listConfigurationSets, 115](#)
- [listConfigurationProperties, 116](#)
- [listConfigurations, 118](#)
- [listConfigurationUserPermissions, 120](#)
- [refreshConfiguration, 121](#)
- [setConfigurationPermissions, 123](#)
- [setConfigurationProperties, 125](#)
- [updateConfiguration, 127](#)

createConfiguration

Importe les informations de cluster directement d'un cluster ou d'un fichier d'archive de cluster.

La configuration de cluster est un objet du domaine qui contient des informations de configuration sur le cluster de calcul.

La syntaxe de la commande de cluster infacmd createConfiguration est la suivante :

```
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|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]
```

Le tableau suivant décrit les options et arguments de la commande de cluster infacmd createConfiguration :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP ou si vous importez des propriétés directement du cluster. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConfigurationName -cn	Nom de la configuration du cluster	Requis. Le nom de la configuration du cluster doit respecter les critères suivants : <ul style="list-style-type: none"> - Unique dans le domaine - Ne peut pas dépasser 128 caractères. - Ne peut pas contenir d'espaces blancs ou les caractères spéciaux suivants : <ul style="list-style-type: none"> - ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? / Les valeurs ne sont pas sensibles à la casse.
-DistributionType -distType	Distribution	Requis. L'un des types de distribution suivants : <ul style="list-style-type: none"> - CDH. Cloudera CDH. - EMR. Amazon EMR. - HDI. Azure HDInsight. - HDP. Hortonworks HDP. - MAPR - DATABRICKS Les valeurs ne sont pas sensibles à la casse.
-DistributionVersion -dv	Version de distribution	Facultatif. Spécifiez une version de distribution autre que la version par défaut. Il existe une version par défaut pour chaque distribution. Utilisez l'option dv pour spécifier une version prise en charge différente à appliquer à la configuration du cluster. La valeur par défaut est la version de distribution la plus récente prise en charge par Data Engineering.
-ClusterManagerUri -uri	URI du gestionnaire de cluster	Obligatoire pour importer directement du cluster. URI de l'interface Web de configuration de cluster.
-ClusterManagerUser -cmu	Utilisateur du gestionnaire de cluster	Obligatoire pour importer directement du cluster. Nom d'utilisateur du compte utilisé pour se connecter à l'interface Web de configuration de cluster.
-ClusterManagerPassword -cmp	Mot de passe du gestionnaire de cluster	Obligatoire pour importer directement du cluster. Mot de passe du compte utilisé pour se connecter à l'interface Web de configuration de cluster.
-ClusterName -cln	Nom de cluster	Obligatoire si le gestionnaire de cluster gère plusieurs clusters. Si vous ne spécifiez pas de nom de cluster, l'assistant importe les informations basées sur le cluster par défaut.

Option	Argument	Description
-FilePath -path	Chemin d'accès et nom de fichier pour l'emplacement du fichier d'archive.	Obligatoire pour importer des informations concernant le cluster à partir d'un fichier. Chemin et nom du fichier d'archive qui contient les informations de cluster.
-createConnections -cc	True False	Facultatif. Indique s'il faut créer des connexions associées à la configuration du cluster. La valeur par défaut est False.

createConfigurationWithParams

Crée une configuration de cluster via les paramètres de cluster que vous spécifiez dans la ligne de commande.

La configuration de cluster est un objet du domaine qui contient des informations de configuration sur le cluster de calcul.

La commande `infacmd cluster createConfigurationWithParams` utilise la syntaxe suivante :

```
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|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.
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd cluster createConfigurationWithParams` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP ou si vous importez des propriétés directement du cluster. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConfigurationName -cn	Nom de la configuration de la grappe	Requis. Le nom de la configuration du cluster doit respecter les critères suivants : <ul style="list-style-type: none"> - Unique dans le domaine - Ne peut pas dépasser 128 caractères. - Ne peut pas contenir d'espaces blancs ou les caractères spéciaux suivants : ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? / Les valeurs ne sont pas sensibles à la casse.
-DistributionType -distType	Distribution	Obligatoire. L'un des types de distribution suivants : <ul style="list-style-type: none"> - CDH. Cloudera CDH. - EMR. Amazon EMR. - HDI. Azure HDInsight. - HDP. Hortonworks HDP. - MAPR - DATABRICKS Les valeurs ne sont pas sensibles à la casse.

Option	Argument	Description
-DistributionVersion -dv	Version de distribution	Facultatif. Spécifiez une version de distribution autre que la version par défaut. Il existe une version par défaut pour chaque distribution. Utilisez l'option dv pour spécifier une version prise en charge différente à appliquer à la configuration du cluster. La valeur par défaut est la version de distribution la plus récente que Big Data Management prend en charge.
-Parameters -params	Paramètres	Séparés par un espace sous la forme name=value. Utilisez un guillemet simple pour échapper tout signe égal ou espace dans la valeur. Vous pouvez utiliser l'un des paramètres suivants pour chaque distribution : <ul style="list-style-type: none"> - Databricks : <ul style="list-style-type: none"> - url - accesstoken - clusterid - Tous les autres types de distribution : <ul style="list-style-type: none"> - host - port - username - password - clustername

deleteConfiguration

Supprime une configuration de grappe du domaine.

Vous ne pouvez pas supprimer une configuration de grappe utilisée par un objet de connexion.

La commande de grappe `infacmd deleteConfiguration` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande de grappe `infacmd deleteConfiguration` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, <code>infacmd</code> utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-ConfigurationName -cn	Nom de la configuration de la grappe	Requis. Nom de la configuration de la grappe sur le domaine. Les valeurs ne sont pas sensibles à la casse.
-DeleteConnections -dc	delete_associated_connection	Facultatif. Définissez cette valeur sur True pour supprimer toutes les connexions associées à la configuration de la grappe. La valeur par défaut est False.

clearConfigurationProperties

Efface les valeurs de propriétés remplacées dans l'ensemble de configuration de grappe.

La commande efface les valeurs substituées des propriétés importées et restaure la valeur importée. La commande supprime les propriétés définies par l'utilisateur d'un ensemble de configuration. Pour supprimer une propriété importée, utilisez l'option -del.

Remarque: Lorsque vous supprimez une propriété importée, l'opération d'actualisation restaure la propriété si celle-ci existe sur le cluster.

Par exemple, la commande suivante supprime les propriétés définies par l'utilisateur « foo.bar » et « biz.baz » de l'ensemble core-site.xml de la configuration de cluster CDH1 :

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

La syntaxe de la commande de cluster infacmd clearConfigurationProperties est la suivante :

```
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]
```


Le tableau suivant décrit les options et arguments de la commande de cluster `infacmd clearConfigurationProperties` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, <code>infacmd</code> utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConfigurationName -cn	Nom de la configuration du cluster	Obligatoire. Nom de la configuration du cluster sur le domaine. Les valeurs ne sont pas sensibles à la casse.

Option	Argument	Description
-ConfigurationSet -cs	Configuration set	Nom de l'ensemble de configuration. Entrez le nom du fichier de configuration xml. Par exemple, hdfs-site.xml. Lorsque vous entrez un nom de fichier .xml, la commande renvoie les propriétés et les valeurs de cet ensemble de configuration.
-PropertyNames -pn	property_name	Propriétés par rapport auxquelles exécuter la commande. Lorsque vous incluez une propriété importée, la commande efface une valeur de remplacement. Lorsque vous incluez une propriété définie par l'utilisateur, la commande la supprime. Pour modifier plusieurs propriétés, séparez leur nom par des espaces. Lorsque la propriété n'est pas une propriété définie par l'utilisateur, utilisez l'option -del.
-DeleteProperties -del	delete_properties	Facultatif. Lorsque vous définissez l'option sur TRUE, une propriété importée est supprimée. La valeur par défaut est FALSE.

exportConfiguration

Exporte une configuration de cluster vers un fichier d'archive contenant des fichiers .xml ou un fichier .xml combiné.

Exportez les propriétés qu'un objet de configuration de cluster contient vers un fichier compressé dans un chemin d'accès que vous spécifiez.

Lorsque vous exportez le fichier de configuration de cluster, vous créez une archive .zip.

La commande de cluster `infacmd exportConfiguration` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande de cluster `infacmd exportConfiguration` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, <code>infacmd</code> utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConfigurationName -cn	Nom de la configuration du cluster	Obligatoire. Nom de la configuration du cluster sur le domaine. Les valeurs ne sont pas sensibles à la casse.

Option	Argument	Description
-FilePath -path	Chemin d'accès et nom de fichier pour l'emplacement du fichier à créer.	Obligatoire. Chemin d'accès et nom du fichier compressé à créer en tant qu'archive de la configuration de cluster. Vous pouvez spécifier un chemin d'accès absolu ou relatif pour le nom de fichier. Incluez un suffixe .zip ou .tar.
-IncludeSensitive -is	include_sensitive_properties	Facultatif. Définissez cette valeur sur TRUE pour exporter les propriétés sensibles. Vous devez disposer d'une autorisation d'écriture sur la configuration de cluster pour les inclure dans l'exportation. La valeur par défaut est FALSE.

listAssociatedConnections

Répertorie les connexions par type associé à la configuration de grappe spécifiée.

La commande répertorie les résultats par type de connexion.

La commande de grappe infacmd listAssociatedConnections utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments de la grappe infacmd listAssociatedConnections :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConfigurationName -cn	Nom de la configuration de la grappe	Requis. Nom de la configuration de la grappe sur le domaine. Les valeurs ne sont pas sensibles à la casse.

listConfigurationGroupPermissions

Répertorie les autorisations d'un groupe sur une configuration de grappe.

Le résultat de commande inclut les autorisations de groupe et le domaine de sécurité auquel appartient le groupe.

La commande de cluster infacmd listConfigurationGroupPermissions utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande de cluster `infacmd listConfigurationGroupPermissions` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, <code>infacmd</code> utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConfigurationName -cn	Nom de la configuration de la grappe	Requis. Nom de la configuration de la grappe sur le domaine. Les valeurs ne sont pas sensibles à la casse.

Option	Argument	Description
-Direct	Détermine si vous répertoriez des autorisations directes ou effectives.	Facultatif. Détermine si vous répertoriez les autorisations que l'administrateur a directement accordées à la configuration de cluster. Spécifiez l'une des valeurs suivantes : - Directe. Autorisations que l'administrateur a directement accordées au groupe. - Effective. Toutes les autorisations du groupe, y compris les autorisations directes et héritées. La valeur par défaut est Effective.
GroupFilter -groups	Filtre groupe	Facultatif. Répertorie le groupe ou les groupes pour lesquels afficher les résultats. Si vous ne spécifiez aucun groupe, la commande affiche les résultats pour tous les groupes par défaut. Séparez les noms de groupe par des espaces.

listConfigurationSets

Répertorie les jeux de configuration qu'une configuration de cluster contient.

La commande de cluster infacmd listConfigurationSets utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments de la commande de cluster infacmd listConfigurationSets :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConfigurationName -cn	Nom de la configuration de la grappe	Requis. Nom de la configuration de la grappe sur le domaine. Les valeurs ne sont pas sensibles à la casse.

listConfigurationProperties

Répertorie les propriétés et les valeurs actives d'un ensemble de configuration.

La syntaxe de la commande de cluster infacmd listConfigurationProperties est la suivante :

```
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
```


Le tableau suivant décrit les options et arguments de la commande de cluster infacmd
listConfigurationProperties :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-ConfigurationName -cn	Nom de la configuration du cluster	Obligatoire. Nom de la configuration du cluster sur le domaine. Les valeurs ne sont pas sensibles à la casse.
-ConfigurationSet -cs	configuration set	Nom de l'ensemble de configuration. Entrez l'une des options suivantes de l'ensemble de configuration : <ul style="list-style-type: none"> - general. Lorsque vous entrez cette option, la commande renvoie les valeurs de propriété sous la catégorie Général des options de configuration de cluster : <ul style="list-style-type: none"> - Description - Type de distribution - Version de distribution - Heure de la dernière actualisation - Nom du fichier de configuration. xml. Par exemple, hdfs-site.xml. Lorsque vous entrez un nom de fichier .xml, la commande renvoie les propriétés et les valeurs de cet ensemble de configuration.

listConfigurations

Répertorie les configurations de cluster dans le domaine.

La commande de cluster `infacmd listConfigurations` utilise la syntaxe suivante :

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

Le tableau suivant décrit les options et arguments de la commande de cluster `infacmd listConfigurations` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, <code>infacmd</code> utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

listConfigurationUserPermissions

Répertorie les autorisations d'un utilisateur sur une configuration de grappe.

La commande de cluster infacmd listConfigurationUserPermissions utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande de cluster infacmd listConfigurationUserPermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConfigurationName -cn	Nom de la configuration de la grappe	Requis. Nom de la configuration de la grappe sur le domaine. Les valeurs ne sont pas sensibles à la casse.
-Direct	Détermine si vous répertoriez des autorisations directes ou effectives.	Facultatif. Détermine si vous répertoriez les autorisations que l'administrateur a directement accordées à la configuration de cluster. Spécifiez l'une des valeurs suivantes : - Directe. Autorisations que l'administrateur a directement accordées au groupe. - Effective. Toutes les autorisations du groupe, y compris les autorisations directes et héritées. La valeur par défaut est Effective.
UserFilter -users	user_filter	Facultatif. Répertoriez l'utilisateur ou les utilisateurs pour lesquels afficher les résultats. Si vous ne spécifiez pas d'utilisateur, la commande affiche les résultats pour tous les utilisateurs par défaut. Les valeurs ne sont pas sensibles à la casse.

refreshConfiguration

Actualise une configuration de cluster à partir d'un fichier d'archive de cluster ou d'un gestionnaire de cluster distant. Les modifications prennent effet une fois que vous redémarrez le service d'intégration de données.

Met à jour les propriétés de configuration de cluster à partir d'un cluster ou d'un fichier d'archive de cluster. La commande refreshConfiguration met à jour les valeurs de configuration que vous avez importées. Elle n'affecte pas les substitutions que vous avez configurées.

La commande de cluster infacmd refreshConfiguration utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande de cluster infacmd refreshConfiguration :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConfigurationName -cn	Nom de la configuration de la grappe	Requis. Nom de la configuration de la grappe sur le domaine. Les valeurs ne sont pas sensibles à la casse.
-ClusterManagerUri -uri	URI du gestionnaire de cluster	Requis pour importer directement du cluster. URI de l'interface Web de configuration de cluster.
-ClusterManagerUser -cmu	Utilisateur du gestionnaire de cluster	Requis pour importer directement du cluster. Nom d'utilisateur du compte utilisé pour se connecter à l'interface Web de configuration de cluster.
-ClusterManagerPassword -cmp	Mot de passe du gestionnaire de cluster	Requis pour importer directement du cluster. Mot de passe du compte utilisé pour se connecter à l'interface Web de configuration de cluster.
-ClusterName -cln	Nom de cluster	Requis si le gestionnaire de cluster gère plusieurs clusters. Si vous ne spécifiez pas de nom de cluster, l'assistant importe les informations basées sur le cluster par défaut.
-FilePath -path	Chemin d'accès et nom de fichier pour l'emplacement du fichier d'archive.	Requis pour importer des informations concernant le cluster à partir d'un fichier. Chemin d'accès et nom du fichier d'archive contenant les fichiers de configuration *-site.xml du cluster.

setConfigurationPermissions

Définit les autorisations d'un utilisateur ou d'un groupe sur une configuration de grappe suite à la suppression des autorisations précédentes.

Vous permet d'ajouter, de modifier ou de supprimer des autorisations de configuration du cluster pour un utilisateur ou un groupe. Supprime des autorisations précédentes pour l'utilisateur ou le groupe.

Utilisez l'option **-RecipientUserName** ou **-RecipientGroupName**.

Vous pouvez accorder plusieurs autorisations de l'ensemble suivant dans une seule commande : READ, WRITE, EXECUTE, GRANT. Vous ne pouvez accorder que ALL ou NONE séparément.

La commande de cluster infacmd setConfigurationPermissions utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et arguments de la commande de cluster infacmd
setConfigurationPermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConfigurationName -cn	Nom de la configuration de la grappe	Requis. Nom de la configuration de la grappe sur le domaine. Les valeurs ne sont pas sensibles à la casse.
-RecipientUserName -run	recipient_user_name	Requis si vous n'utilisez pas l'option RecipientGroupName. Nom de l'utilisateur auquel accorder l'autorisation.
-RecipientGroupName -rgn	recipient_group_name	Requis si vous n'utilisez pas l'option RecipientUserName. Nom du groupe auquel accorder l'autorisation.
-RecipientSecurityDomain -rsd	recipient_security_domain	Domaine de sécurité auquel appartient l'utilisateur ou le groupe.
-Permissions -p	READ WRITE EXECUTE GRANT ALL NONE	Autorisation(s) à accorder. Pour entrer plusieurs autorisations, séparez-les par un espace.

setConfigurationProperties

Ajoute des propriétés définies par l'utilisateur ou remplace des valeurs de propriété importées.

La commande de grappe infacmd setConfigurationProperties utilise la syntaxe suivante :

```
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_&:
```

Le tableau suivant décrit les options et arguments de la grappe infacmd setConfigurationProperties :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConfigurationName -cn	Nom de la configuration de la grappe	Requis. Nom de la configuration de la grappe sur le domaine. Les valeurs ne sont pas sensibles à la casse.

Option	Argument	Description
-ConfigurationSet -cs	ensemble de configuration	Nom de l'ensemble de configuration. Entrez le nom du fichier de configuration xml. Par exemple, hdfs-site.xml. Lorsque vous entrez un nom de fichier .xml, la commande renvoie les propriétés et les valeurs de cet ensemble de configuration.
-UserProperties -up	Propriétés de l'utilisateur à définir	Paires nom-valeur d'une propriété. Utilisez le caractère égal (=) pour délimiter les paires propriété-valeur. Utilisez les caractères & : pour séparer chaque paire.

Exemples de -UserProperties

Les exemples suivants montrent comment ajouter une propriété d'utilisateur unique, plusieurs paires propriété-valeur ou comment remplacer une propriété d'utilisateur :

Ajouter une propriété d'utilisateur unique

Pour ajouter une propriété d'utilisateur unique, utilisez le caractère égal (=) pour délimiter les paires propriété-valeur. Par exemple, la commande suivante ajoute la propriété foo.bar à l'espace de noms core-site.xml de la configuration de la grappe et attribue à foo.bar la valeur 1 :

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

Ajouter plusieurs paires propriété-valeur

Utilisez le caractère égal (=) pour délimiter les paires propriété-valeur et utilisez & : pour séparer les paires. Par exemple, la commande suivante ajoute la propriété foo.bar à l'espace de noms core-site.xml de la configuration du cluster et attribue à foo.bar une valeur 1. Elle ajoute ensuite la propriété start.interval au même espace de noms et attribue à start.interval une valeur 5 :

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

Remplacer une propriété d'utilisateur

Pour remplacer la valeur d'une propriété d'utilisateur, spécifiez une autre valeur pour la paire propriété-valeur. Par exemple, la commande suivante modifie la propriété fs.trash.interval existante dans l'espace de noms core-site.xml de la configuration de la grappe. La commande remplace la valeur existante et attribue une valeur de 2 :

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

updateConfiguration

Met à jour la version de distribution Hadoop d'une configuration de cluster.

Utilisez l'option -dv pour modifier la version de distribution de la distribution Hadoop d'une configuration de cluster.

La syntaxe de la commande de cluster infacmd updateConfiguration est la suivante :

```
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
```

Le tableau suivant décrit les options et arguments de la commande de cluster infacmd updateConfiguration :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-ConfigurationName -cn	Nom de la configuration du cluster	Obligatoire. Nom de la configuration du cluster sur le domaine. Les valeurs ne sont pas sensibles à la casse.
-DistributionVersion -dv	Version de distribution à migrer.	Obligatoire. Spécifiez une version de distribution différente pour une configuration de cluster. Par exemple, si la version prise en charge par défaut de la distribution Hadoop est 5.13 mais que le cluster est de version 5.12, spécifiez 5.12.

CHAPITRE 12

Référence de commande infacmd CMS

Ce chapitre comprend les rubriques suivantes :

- [CreateAuditTables, 130](#)
- [CreateService, 132](#)
- [DeleteAuditTables, 134](#)
- [ListServiceOptions, 136](#)
- [ListServiceProcessOptions, 138](#)
- [Purge, 139](#)
- [RemoveService, 141](#)
- [ResyncData, 143](#)
- [UpdateServiceOptions, 145](#)
- [UpdateServiceProcessOptions, 148](#)
- [Mise à niveau, 150](#)

CreateAuditTables

Crée des tables d'audit qui contiennent les événements de journal du suivi d'audit pour les tables de référence gérées par le service de gestion du contenu spécifié.

La commande infacmd cms CreateAuditTables utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd cms CreateAuditTables :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de gestion de contenu.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

CreateService

Crée un service de gestion de contenu dans un domaine.

La commande infacmd cms CreateService utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd cms CreateService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de gestion de contenu. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 128 caractères, commencer ou terminer par des espaces ou contenir des retours chariot, des tabulations ou les caractères suivants : / * ? < > "

Option	Argument	Description
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire. La valeur par défaut est 180 secondes.
-NodeName -nn	node_name	Obligatoire. Nom du nœud sur lequel le service de gestion de contenu sera exécuté.
-DataServer -ds	data_service_name	Obligatoire. Nom du service d'intégration de données associé au service de gestion de contenu.
-RepositoryService -rs	repository_service_name	Obligatoire. Service de référentiel modèle à associer au service de gestion de contenu.

Option	Argument	Description
-RepositoryUsername -rsu	repository_user_Name	Obligatoire. Nom d'utilisateur pour la connexion au service de référentiel modèle. Pour effectuer les tâches de gestion des tables de référence dans le référentiel modèle, l'utilisateur identifié dans la propriété doit disposer du rôle d'administrateur du service de référentiel modèle. Les tâches de gestion des tables de référence incluent des opérations de purge sur les tables de référence orphelines.
-RepositoryPassword -rsp	repository_password	Obligatoire. Mot de passe pour se connecter au service de référentiel modèle.
-RepositorySecurityDomain -rssd	_repository_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.
-ReferenceDataLocation -rdl	reference_data_location	Obligatoire. Nom de connexion de la base de données qui stocke des valeurs de données pour les tables de référence définies dans le référentiel modèle. La base de données spécifiée stocke des valeurs de données de référence. Le référentiel modèle stocke des métadonnées pour les tables de référence.
-HttpPort	http_port	Obligatoire. Numéro de port HTTP unique pour le service de gestion de contenu.
-HttpsPort	https_port	Facultatif. Numéro de port HTTPS sur lequel le service s'exécute lorsque vous activez le protocole TLS (Transport Layer Security).
-KeystoreFile -kf	keystore_file_location	Chemin d'accès et nom du fichier entrepôt de clés contenant les clés et les certificats requis si vous activez TLS et utilisez le protocole HTTPS pour le service.
-KeystorePassword> -kp	keystore_password	Obligatoire si vous activez le protocole TLS et que vous utilisez des connexions HTTPS pour le service. Mot de passe en texte clair pour le fichier entrepôt de clés.

DeleteAuditTables

Supprime les tables de suivi d'audit pour le service de gestion du contenu spécifié.

La commande `infacmd cms DeleteAuditTables` utilise la syntaxe suivante :

```

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]
```

Le tableau suivant décrit les options et arguments d'infacmd cms DeleteAuditTables :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de gestion de contenu.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

ListServiceOptions

Répertorie les options pour un service de gestion du contenu.

La commande `infacmd cms ListServiceOptions` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd cms ListServiceOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de gestion de contenu.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

ListServiceProcessOptions

Répertorie les options d'un processus de service de gestion du contenu.

La commande infacmd cms ListServiceProcessOptions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments de la commande cms ListServiceProcessOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	Service_name	Obligatoire. Nom du service de gestion de contenu.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	Security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
NodeName -nn	node_name	Obligatoire. Nom du nœud d'exécution du processus de service.

Purge

Supprime de l'entrepôt de données de référence toute table de référence qui n'est plus associée à un objet de table de référence dans le référentiel modèle.

Lorsque vous exécutez la commande `infacmd cms Purge`, le service de gestion de contenu identifie les tables qui stockent des données pour les objets de la table de référence dans le référentiel modèle associé. Le service de gestion de contenu supprime toutes les autres tables de l'entrepôt de données et génère une liste des tables supprimées. Exécutez la commande `infacmd cms Purge` sur le service de gestion de contenu principal pour le référentiel modèle.

Remarque: Pour éviter la perte accidentelle de données, l'opération de purge ne supprime pas les tables si le référentiel modèle ne contient pas d'objet de table de référence.

Avant d'exécuter `infacmd cms Purge`, vérifiez les conditions préalables suivantes :

- Le nom d'utilisateur que vous spécifiez dans la commande a le privilège de service de gestion sur le domaine.
- L'utilisateur du référentiel modèle que le service de gestion du contenu spécifie a le rôle d'administrateur sur le service du référentiel modèle.
- Tous les services d'intégration de données associés au référentiel modèle sont disponibles.
- Il n'y a pas d'opérations de données en cours dans l'entrepôt de données de référence.

- L'entrepôt de données de référence stocke les données des objets de la table de référence dans un seul référentiel modèle.

La commande infacmd cms Purge utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd cms Purge :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de gestion de contenu. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 128 caractères, commencer ou terminer par des espaces ou contenir des retours chariot, des tabulations ou les caractères suivants : / * ? < > "
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire. La valeur par défaut est 180 secondes.

RemoveService

Supprime le service de gestion du contenu du domaine. Avant de supprimer le service, vous devez le désactiver.

La commande infacmd CMS RemoveService utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd cms RemoveService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service que vous souhaitez supprimer. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

ResyncData

Synchronise des fichiers modèles probabilistes et classificateurs entre un ordinateur du service de gestion de contenu et l'ordinateur du service de gestion de contenu principal du domaine. La commande ResyncData met à jour les fichiers de l'ordinateur du service de gestion de contenu que vous spécifiez avec les fichiers de l'ordinateur du service de gestion de contenu principal.

La commande synchronise tout fichier enregistré sur l'ordinateur du service de gestion de contenu principal à la date et l'heure que vous avez indiqué. Vous exécutez la commande ResyncData pour un seul type de fichier de modèle. Pour synchroniser les fichiers modèles probabilistes et classificateurs, vous devez exécuter la commande deux fois.

Lorsque vous exécutez la commande infacmd cms ResyncData, vous devez avoir les autorisations d'accès aux deux ordinateurs du service de gestion de contenu. Informatica Administrator définit les autorisations d'accès aux services.

La commande infacmd cms ResyncData utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd cms ResyncData :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	Service_name	Obligatoire. Nom du service de gestion de contenu. La commande copie les fichiers sur l'ordinateur qui héberge le service.

Option	Argument	Description
-UserName -un	user_name	<p>Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>
-Password -pd	mot de passe	<p>Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p> <p>.</p>
-SecurityDomain -sdn	Security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>

Option	Argument	Description
-Type -t	type	Obligatoire. Identifie le type de fichier de données qu'il faut copier de l'ordinateur du service de gestion de contenu principal. Entrez l'une des options suivantes : - NER. Spécifie les fichiers de données des modèles probabilistes. - Classeur Spécifie les fichiers de données des modèles classificateurs
-StartTime -st	start_time	Obligatoire. Identifie les fichiers qu'il faut copier de l'ordinateur du service de gestion de contenu principal vers l'ordinateur du service de gestion de contenu que vous spécifiez dans la propriété ServiceName. La commande ne copie aucun fichier avec un horodatage antérieur à la valeur StartTime. La commande utilise le système d'horloge de l'ordinateur du service de gestion de contenu principal pour déterminer le temps. Entrez la date au format du paramètre régional par défaut.

UpdateServiceOptions

Met à jour le service de gestion du contenu avec des options qui sont intégrées dans la version actuelle. Pour afficher les options actuelles, exécutez la commande `infacmd cms ListServiceOptions`.

La syntaxe de la commande `infacmd cms UpdateServiceOptions` est la suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd cms UpdateServiceOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de gestion de contenu.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Options -o	options	Obligatoire. Entrez chaque option et valeur à mettre à jour. Séparez chaque option par un espace. Pour afficher les options de l'application, exécutez la commande infacmd cms ListServiceOptions.

Options de nom d'utilisateur et de mot de passe

Vous pouvez utiliser l'option UpdateServiceOptions -o pour mettre à jour le nom d'utilisateur et le mot de passe que le service de gestion du contenu utilise pour se connecter au service de référentiel modèle. Utilisez les options DataServiceOptions.RepositoryUsername et DataServiceOptions.RepositoryPassword pour mettre à jour les valeurs de nom d'utilisateur et de mot de passe. Vous pouvez également définir les options dans Informatica Administrator.

Options de données de référence

Vous pouvez utiliser l'option UpdateServiceOptions -o pour mettre à jour les paramètres de répertoires et de bases de données suivants pour les données de référence :

- Utilisez l'option FileTransferOptions.TempLocation pour identifier le répertoire intermédiaire de données de référence. Le service de gestion du contenu utilise le répertoire d'activation de données pour organiser les données qu'il ajoute à une table de référence.
- Utilisez l'option DataServiceOptions.ReferenceDataLocation pour identifier la connexion à la base de données de référence. La base de données de référence stocke les valeurs des tables de référence à sélectionner dans le référentiel modèle.
- Utilisez l'option DataServiceOptions.RefDataLocationSchema pour spécifier le schéma qui identifie les tables de données de référence dans la base de données de référence.

Si vous ne spécifiez pas un schéma de table de référence sur le service de gestion de contenu, le service utilise le schéma spécifié par la connexion à la base de données. Si vous ne spécifiez pas un schéma sur le service de gestion de contenu ou sur la connexion à la base de données, le service utilise le schéma de base de données par défaut.

Vous pouvez également définir les options dans Informatica Administrator.

Remarque: Établissez la base de données et le schéma que le service de gestion de contenu utilisera pour les données de référence avant de créer une table de référence gérée.

UpdateServiceProcessOptions

Met à jour les options pour un processus de service de gestion du contenu. Pour afficher les options courantes, exécutez la commande `infacmd cms ListServiceProcessOptions`.

La syntaxe de la commande `infacmd cms UpdateServiceProcessOptions` est la suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'`infacmd cms UpdateServiceProcessOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de gestion de contenu.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
NodeName -nn	node_name	Obligatoire. Nom du nœud d'exécution du processus de service.
-Options -o	options	Obligatoire. Entrez chaque option et valeur à mettre à jour. Séparez chaque option par un espace. Pour afficher les options de l'application, exécutez la commande infacmd cms ListServiceProcessOptions.

Options d'analyse de correspondance d'identité

Vous pouvez utiliser l'option UpdateServiceProcessOptions -o pour mettre à jour les propriétés suivantes pour l'analyse de correspondance d'identité :

- IdentityOptions.IdentityReferenceDataLocation. Spécifie l'emplacement des fichiers de population d'identités.
- IdentityOptions.IdentityCacheDir. Spécifie l'emplacement du répertoire de cache utilisé dans l'analyse de correspondance d'identité.
- IdentityOptions.IdentityIndexDir. Spécifie l'emplacement du répertoire clé de l'index utilisé dans l'analyse de correspondance d'identité.

Vous pouvez aussi définir les propriétés dans Informatica Administrator.

Mise à niveau

Met à niveau la configuration du service de gestion du contenu. Exécutez la commande `infacmd cms Upgrade` lorsque vous effectuez une mise à niveau vers la version actuelle d'Informatica Data Quality.

La commande `infacmd cms Upgrade` utilise la syntaxe suivante :

```
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]
```

La commande `infacmd cms Upgrade` vérifie la configuration de service du domaine et les options de service suivantes :

Service de gestion du contenu principal

La commande `Upgrade` vérifie que le référentiel modèle du domaine utilise un service de gestion du contenu principal. Si le service de référentiel modèle ne spécifie pas un service de gestion du contenu principal, la commande `Upgrade` définit le service actuel comme étant le service de gestion du contenu principal. Par défaut, le premier service de gestion du contenu pour se connecter à un service de référentiel modèle devient le service de gestion du contenu principal.

Service de référentiel modèle

La commande `Upgrade` utilise le service d'intégration de données associé au service de gestion du contenu pour identifier le service de référentiel modèle dans le domaine.

La commande `Upgrade` vérifie que le service de gestion du contenu a un nom d'utilisateur, un mot de passe et un domaine de sécurité valides pour se connecter au service de référentiel modèle. Si ces options ne sont pas définies, la commande `Upgrade` utilise les valeurs de nom d'utilisateur, mot de passe et domaine de sécurité du service d'intégration de données associé pour se connecter au service de référentiel modèle.

Emplacement des données de référence

La commande `Upgrade` vérifie que le service de gestion du contenu indique un emplacement pour les données de référence. Si le service ne spécifie pas un emplacement pour les données de référence, la commande `Upgrade` définit l'emplacement de la base de données temporaire définie dans le Service Analyst.

Le tableau suivant décrit les options et arguments d'`infacmd cms Upgrade` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de gestion de contenu.

Option	Argument	Description
-UserName -un	user_name	<p>Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>
-Password -pd	mot de passe	<p>Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p>
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>

CHAPITRE 13

référence de commande infacmd dis

Ce chapitre comprend les rubriques suivantes :

- [AddParameterSetEntries, 153](#)
- [BackupApplication, 155](#)
- [CancelDataObjectCacheRefresh, 157](#)
- [CreateService, 159](#)
- [compareMapping, 162](#)
- [compareObject, 166](#)
- [DeleteParameterSetEntries, 170](#)
- [deployObjectsToFile, 172](#)
- [DeployApplication, 176](#)
- [disableMappingValidationEnvironment, 178](#)
- [enableMappingValidationEnvironment, 180](#)
- [ListApplicationObjectPermissions, 183](#)
- [ListApplicationObjects, 185](#)
- [ListApplicationOptions, 187](#)
- [ListApplicationPermissions, 189](#)
- [ListApplications, 190](#)
- [ListComputeOptions, 192](#)
- [ListDataObjectOptions, 193](#)
- [ListMappingEngines, 195](#)
- [ListParameterSetEntries, 198](#)
- [ListParameterSetObjects, 200](#)
- [ListParameterSets, 201](#)
- [listPatchNames, 203](#)
- [ListSequenceObjectProperties, 204](#)
- [ListSequenceObjects, 206](#)
- [ListServiceOptions, 208](#)
- [ListServiceProcessOptions, 210](#)
- [PurgeDataObjectCache, 211](#)

- [PurgeResultSetCache, 213](#)
- [queryDesignTimeObjects, 215](#)
- [queryRunTimeObjects, 217](#)
- [RefreshDataObjectCache, 218](#)
- [RenameApplication, 220](#)
- [replaceMappingHadoopRuntimeConnections, 222](#)
- [RestoreApplication, 224](#)
- [SetApplicationPermissions, 226](#)
- [SetApplicationObjectPermissions, 228](#)
- [setMappingExecutionEnvironment, 230](#)
- [SetSequenceState, 232](#)
- [StartApplication, 235](#)
- [StopApplication, 236](#)
- [stopBlazeService, 238](#)
- [tag, 241](#)
- [UndeployApplication, 249](#)
- [UpdateApplication, 250](#)
- [UpdateApplicationOptions, 252](#)
- [UpdateComputeOptions, 254](#)
- [UpdateDataObjectOptions, 256](#)
- [UpdateParameterSetEntries, 259](#)
- [UpdateServiceOptions , 261](#)
- [UpdateServiceProcessOptions , 275](#)
- [Règles et directives, 278](#)

AddParameterSetEntries

Ajoute les entrées à un ensemble de paramètres. Exécutez cette commande pour ajouter des paramètres d'un mappage ou d'un flux de travail déployé en tant qu'application.

La commande infacmd dis AddParameterSetEntries utilise la syntaxe suivante :

```
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

Le tableau suivant décrit les options et les arguments de la commande infacmd dis
AddParameterSetEntries :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel est déployée l'application.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application	Requis. Nom de l'application qui contient l'ensemble de paramètres.
parametersetname -ps	nom de l'ensemble de paramètres	Requis. Nom de l'ensemble de paramètres.
-projectScope -prs	portée du projet	Requis. Chemin du mappage ou du flux de travail qui contient les paramètres. Pour un mappage M1 dans un projet P1 et un dossier F1, le chemin est P1/F1/mapping/M1.
-paramNames -pnv	noms de paramètre	Requis. Paramètre des paires nom-valeur séparées par un espace. Placez les paires nom-valeur entre guillemets doubles. Placez chaque valeur entre des guillemets simples. Utilisez la syntaxe suivante : "parm1='valueA'" "parm2='valueB'" "parm3='valueC" . Vous pouvez inclure des espaces dans une valeur de paramètre. Vous pouvez inclure une apostrophe (') ou un signe deux-points (:) dans la valeur si vous échappez le caractère à l'aide d'une barre oblique inversée (\). 'C: \directory'

BackupApplication

Sauvegarde une application déployée depuis un service d'intégration de données vers un fichier XML.

Le fichier de sauvegarde contient tous les paramètres des propriétés pour l'application. Vous pouvez restaurer l'application dans un autre service d'intégration de données. Vous devez arrêter l'application avant de la sauvegarder.

La commande infacmd dis BackupApplication utilise la syntaxe suivante :

```
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

Le tableau suivant décrit les options et arguments d'infacmd dis BackupApplication :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données dans lequel est déployée l'application.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-Application -a	application	Obligatoire. Nom de l'application à sauvegarder.
Nom du fichier -f	file_name	Obligatoire. Nom et chemin du fichier de sauvegarde de l'application.

CancelDataObjectCacheRefresh

Arrête la dernière demande d'actualisation du cache d'objet de données logique. Si le mappage du cache est en cours d'exécution, la commande arrête la demande actuelle d'actualisation du cache d'objet de données logique. Les futures demandes régulières d'actualisation du cache d'objet de données logique ne seront pas affectées.

La commande infacmd dis CancelDataObjectCacheRefresh utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments de la commande `infacmd dis CancelDataObjectCacheRefresh` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données.

Option	Argument	Description
Application -a	application	Obligatoire. Nom de l'application.
-Folder -f	dossier	Dossier dans l'application qui contient l'objet de données.
-DataObject -do	data_model.data_object	Obligatoire. Nom de l'objet de données logique. Le nom doit respecter la syntaxe suivante : <data_model>.<data_object>

CreateService

Crée un service d'intégration de données. Par défaut, le service d'intégration de données est activé lorsque vous le créez.

La commande infacmd dis CreateService utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd dis CreateService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 230 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-NodeName -nn	node_name	Obligatoire si vous ne spécifiez pas le nom de la grille. Nœud d'exécution du service d'intégration de données. Vous pouvez exécuter le service d'intégration de données sur un nœud ou une grille.
-GridName -gn	grid_name	Obligatoire si vous ne spécifiez pas le nom du nœud. Grille d'exécution du service d'intégration de données. Vous pouvez exécuter le service d'intégration de données sur un nœud ou une grille.
-BackupNodes -bn	node_name1,node_name2,...	Facultatif. Nœuds sur lesquels le processus de service peut s'exécuter lorsque le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.
-RepositoryService -rs	model_repository_service_name	Service de référentiel modèle qui stocke les métadonnées d'exécution requises pour exécuter les mappages et les services de données SQL.
-RepositoryUserName -rsun	model_repository_user_name	Nom d'utilisateur pour l'accès au service de référentiel modèle.
-RepositoryPassword -rspd	model_repository_password	Mot de passe utilisateur pour l'accès au service de référentiel modèle.
-RepositorySecurityDomain -rssdn	model_repository_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur du référentiel modèle.
-HttpPort	http_port	Requis si vous ne spécifiez pas de port HTTPS. Numéro de port HTTP unique utilisé pour chaque processus de service d'intégration de données. Après avoir créé le service, vous pouvez définir des numéros de port différents pour chaque processus de service d'intégration de données. La valeur par défaut est 8095.
-HttpsPort	https_port	Requis si vous ne spécifiez pas un port HTTP. Numéro de port HTTPS unique utilisé pour chaque processus de service d'intégration de données. Après avoir créé le service, vous pouvez définir des numéros de port différents pour chaque processus de service d'intégration de données.

Option	Argument	Description
-KeystoreFile -kf	keystore_file_location	Chemin d'accès et nom du fichier entrepôt de clés contenant les clés et les certificats obligatoires si vous utilisez le protocole HTTPS pour le service d'intégration de données. Vous pouvez créer un fichier entrepôt de clés avec un utilitaire keytool. keytool est un utilitaire qui génère et stocke des paires de clés privées et publiques et les certificats associés dans un fichier entrepôt de clés. Vous pouvez utiliser le certificat auto-signé ou un certificat signé par une autorité de certification. Si vous exécutez le service d'intégration de données dans une grille, le fichier entrepôt de clés sur chaque nœud de la grille doit contenir les mêmes clés.
-KeystorePassword -kp	keystore_password	Mot de passe du fichier entrepôt de clés.
-httpProtocolType -pt	http_protocol_type	<p>Protocole de sécurité que le service d'intégration de données utilise. Entrez l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> - HTTP. Les demandes effectuées auprès du service doivent utiliser une URL HTTP. - HTTPS. Les demandes effectuées auprès du service doivent utiliser une URL HTTPS. - Les deux. Les demandes effectuées auprès du service peuvent utiliser une URL HTTP ou HTTPS. <p>Lorsque vous définissez le type de protocole HTTP sur HTTPS ou les deux, vous devez activer TLS (Transport Layer Security) pour le service.</p> <p>Vous pouvez également activer le protocole TLS pour chaque service Web déployé vers une application. Lorsque vous activez le protocole HTTPS pour le service d'intégration de données et activez le protocole TLS pour le service Web, celui-ci utilise une URL HTTPS. Lorsque vous activez le protocole HTTPS pour le service d'intégration de données et n'activez pas le protocole TLS pour le service Web, celui-ci peut utiliser une URL HTTP ou HTTPS. Si vous activez TLS pour un service Web et n'activez pas le protocole HTTPS pour le service d'intégration de données, le service Web ne démarre pas.</p> <p>La valeur par défaut est HTTP.</p>

compareMapping

Compare deux mappages interrogés.

Interrogez les objets pour comparer des propriétés, des propriétés de transformations et des ports au sein de transformations.

Pour interroger les objets en phase de conception, spécifiez le référentiel modèle en phase de conception. Pour interroger des objets d'exécution, ne spécifiez aucun référentiel modèle. La requête utilise le référentiel modèle associé au service d'intégration de données qui exécute la demande.

Avis d'obsolescence: À compter de la version 10.5, la commande infacmd dis compareMapping est obsolète et sera supprimée dans une version ultérieure. Si vous utilisez des scripts basés sur la commande infacmd dis compareMapping, Informatica vous recommande de les mettre à jour à l'aide de la nouvelle commande

infacmd dis compareObject. La fonctionnalité obsolète est prise en charge, mais Informatica prévoit d'interrompre la prise en charge dans une version ultérieure. Informatica vous demande de passer à une fonctionnalité différente avant de l'interrompre.

La syntaxe de la commande infacmd dis compareMapping est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd dis compareMapping :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	DIS_service_name	Requis. Nom du service d'intégration de données.
-UserName -un	DIS_user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.

Option	Argument	Description
-Password -pd	DIS_password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	DIS_security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.
-sourceRepositoryService -srcrs	source_MRS_name	Facultatif. Nom du service de référentiel modèle pour l'objet source.
-sourceRepositoryUserName -srcrsun	source_MRS_user_name	Facultatif. Nom d'utilisateur du service de référentiel modèle utilisé pour accéder à l'objet source. Vous pouvez définir le nom d'utilisateur avec l'option -srcrsun ou la variable d'environnement INFA_SOURCE_REPOSITORY_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -srcrsun est prioritaire.
-sourceRepositoryPassword -srcrspd	source_MRS_password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -srcrspd ou la variable d'environnement INFA_SOURCE_REPOSITORY_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -srcrspd est prioritaire.

Option	Argument	Description
- sourceRepositorySecurityDomain -srcrssdn	source_MRS_security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -srcrssdn ou la variable d'environnement INFA_DEFAULT_SOURCE_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -srcrssdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.
-sourceQuery -srcq	source_query	Requis. Chaîne qui interroge l'objet source. Pour plus d'informations, voir "Requêtes" à la page 280
-targetRepositoryService -tgtrs	target_MRS_name	Facultatif. Nom du service de référentiel modèle pour l'objet cible.
-targetRepositoryUserName -tgtrsun	target_MRS_user_name	Facultatif. Nom d'utilisateur du service de référentiel modèle utilisé pour accéder à l'objet cible. Vous pouvez définir le nom d'utilisateur avec l'option -tgtrsun ou la variable d'environnement INFA_TARGET_REPOSITORY_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -tgtrsun est prioritaire.
-targetRepositoryPassword -tgtrspd	target_MRS_password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -tgtrspd ou la variable d'environnement INFA_TARGET_REPOSITORY_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -tgtrspd est prioritaire.

Option	Argument	Description
-targetRepositorySecurityDomain -tgttrssdn	target_MRS_security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -tgttrssdn ou la variable d'environnement INFA_DEFAULT_TARGET_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -tgttrssdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.
-targetQuery -tgtq	target_query	Obligatoire. Chaîne qui interroge l'objet cible. Pour plus d'informations, voir "Requêtes" à la page 280
-TimeZone -tz	time_zone	Facultatif. Par défaut, la commande utilise le fuseau horaire de la machine qui exécute le processus du service d'intégration de données. Pour obtenir une liste des fuseaux horaires valides, reportez-vous à la classe java.time.ZoneID.

compareObject

Compare deux objets interrogés.

Interrogez les objets pour comparer des propriétés d'objet, des propriétés de transformation et des ports au sein de transformations entre le service d'intégration de données et le service de référentiel modèle. Vous pouvez comparer des objets des manières suivantes :

- D'une phase de conception à une autre au sein d'un même domaine
- D'une phase de conception à une phase d'exécution au sein d'un même domaine
- D'une phase d'exécution à une autre au sein d'un même domaine
- D'une phase de conception à une autre dans des domaines différents
- D'une phase d'exécution à une autre dans des domaines différents

Pour interroger des objets en phase de conception, spécifiez le service de référentiel modèle. Pour interroger des objets d'exécution, spécifiez un service d'intégration de données. Si vous ne spécifiez aucun service, l'API exécute la requête dans les objets d'exécution sur le service d'intégration de données qui héberge l'API.

La syntaxe de la commande infacmd dis compareObject est la suivante :

```
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|-tgtnd> 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]

```

Le tableau suivant décrit les options et les arguments de la commande `infacmd dis compareMapping` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	DIS_service_name	Requis. Nom du service d'intégration de données.
-UserName -un	DIS_user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.

Option	Argument	Description
-Password -pd	DIS_password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	DIS_security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.
-sourceDomainName -srcdn	source_domain_name	Requis. Nom du domaine de l'objet source.
-sourceRepositoryService -srcrs	source_MRS_name	Facultatif. Nom du service de référentiel modèle pour l'objet source.
-sourceDataIntegrationService -srcdis	source_DIS_name	Facultatif. Nom du service d'intégration de données de l'objet source.
-sourceRepositoryUserName -srcrsun	source_MRS_user_name	Facultatif. Nom d'utilisateur du service de référentiel modèle utilisé pour accéder à l'objet source. Vous pouvez définir le nom d'utilisateur avec l'option -srcrsun ou la variable d'environnement INFA_SOURCE_REPOSITORY_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -srcrsun est prioritaire.
-sourceRepositoryPassword -srcrspd	source_MRS_password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -srcrspd ou la variable d'environnement INFA_SOURCE_REPOSITORY_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -srcrspd est prioritaire.

Option	Argument	Description
- sourceRepositorySecurityDomain -srcrssdn	source_MRS_security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -srcrssdn ou la variable d'environnement INFA_DEFAULT_SOURCE_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -srcrssdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.
-sourceQuery -srcq	source_query	Requis. Chaîne qui interroge l'objet source. Pour plus d'informations, consultez la section "Requêtes" à la page 280
-targetDomainName -tgtdn	target_domain_name	Requis. Nom du domaine de l'objet cible.
-targetRepositoryService -tgtrs	target_MRS_name	Facultatif. Nom du service de référentiel modèle pour l'objet cible.
-targetDataIntegrationService -tgtdis	target_DIS_name	Facultatif. Nom du service d'intégration de données de l'objet cible.
-targetRepositoryUserName -tgtrsun	target_MRS_user_name	Facultatif. Nom d'utilisateur du service de référentiel modèle utilisé pour accéder à l'objet cible. Vous pouvez définir le nom d'utilisateur avec l'option -tgtrsun ou la variable d'environnement INFA_TARGET_REPOSITORY_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -tgtrsun est prioritaire.
-targetRepositoryPassword -tgtrspd	target_MRS_password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -tgtrspd ou la variable d'environnement INFA_TARGET_REPOSITORY_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -tgtrspd est prioritaire.

Option	Argument	Description
-targetRepositorySecurityDomain -tgtssdn	target_MRS_security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -tgtssdn ou la variable d'environnement INFA_DEFAULT_TARGET_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -tgtssdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.
-targetQuery -tgtq	target_query	Requis. Chaîne qui interroge l'objet cible. Pour plus d'informations, consultez le chapitre "Requêtes" à la page 280
-TimeZone -tz	time_zone	Facultatif. Par défaut, la commande utilise le fuseau horaire de la machine qui exécute le processus du service d'intégration de données. Pour obtenir une liste des fuseaux horaires valides, reportez-vous à la classe java.time.ZoneID.

DeleteParameterSetEntries

Supprime les entrées d'un ensemble de paramètres. Exécutez cette commande pour supprimer des entrées de l'ensemble de paramètres d'un mappage ou d'un flux de travail déployé en tant qu'application. Vous pouvez supprimer des entrées spécifiques ou supprimer toutes les entrées.

Si l'un des paramètres que vous voulez supprimer n'existe pas dans l'ensemble de paramètres, la commande infacmd renvoie un message d'avertissement. Le message indique que le paramètre n'est pas supprimé, car il ne se trouve pas dans l'ensemble de paramètres.

La commande infacmd dis DeleteParameterSetEntries utilise la syntaxe suivante :

```

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.

Le tableau suivant décrit les options et les arguments de la commande infacmd deleteParameterSetEntries :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel est déployée l'application.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application	Requis. Nom de l'application qui contient l'ensemble de paramètres.
parametersetname -ps	nom de l'ensemble de paramètres	Requis. Nom de l'ensemble de paramètres.
-projectScope -prs	portée du projet	Requis. Chemin du mappage ou du flux de travail qui contient les paramètres. Pour un mappage M1 dans un projet P1 et un dossier F1, le chemin est P1/F1/mapping/M1.
-paramNames -pnr	noms de paramètre	Requis. Noms d'entrée de l'ensemble de paramètres à supprimer, séparés par un espace. Pour supprimer tous les paramètres, utilisez l'option -all au lieu de cette option.
-all	all	Supprimer tous les paramètres de l'ensemble de paramètres.

deployObjectsToFile

Déploye les objets en phase de conception dans un fichier d'archive de correctif d'application.

Interrogez les objets que vous voulez mettre en package dans le fichier d'archive de correctif d'application. Vous pouvez utiliser le fichier pour effectuer les tâches suivantes :

- Déployer une application incrémentielle dans un service d'intégration de données pour la première fois en utilisant infacmd dis ["DeployApplication" à la page 176](#).
- Mettre à jour une application incrémentielle déployée en utilisant infacmd tools ["patchApplication" à la page 1185](#).
- Redéployer une application incrémentielle en utilisant infacmd dis ["UpdateApplication" à la page 250](#).

Remarque: La commande infacmd dis deployObjectsToFile crée un fichier d'archive de correctif d'application sur n'importe quel nœud d'une grille. Vous pouvez également afficher les détails du nœud dans le rapport de requête.

La syntaxe de la commande infacmd dis deployObjectsToFile est la suivante :

```

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]

```

Le tableau suivant décrit les options et les arguments de la commande `infacmd dis deployObjectsToFile` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	DIS_service_name	Requis. Nom du service d'intégration de données.
-UserName -un	DIS_user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.

Option	Argument	Description
-Password -pd	DIS_password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	DIS_security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.
-RepositoryService -rs	MRS_service_name	Requis. Nom du service de référentiel modèle.
-RepositoryUserName -rsun	MRS_user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -rsun ou la variable d'environnement INFA_REPOSITORY_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -rsun est prioritaire.

Option	Argument	Description
-RepositoryPassword -rspd	MRS_password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -rspd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -rspd est prioritaire.
-RepositorySecurityDomain -rssdn	MRS_security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -rssdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -rssdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.
-Query -q	query	Requis. Chaîne qui interroge l'objet. Pour plus d'informations, voir "Requêtes" à la page 280
-TimeZone -tz	time_zone	Facultatif. Par défaut, la commande utilise le fuseau horaire de la machine qui exécute le processus du service d'intégration de données. Pour obtenir une liste des fuseaux horaires valides, reportez-vous à la classe java.time.ZoneID.
-PatchName -ptn	patch_name	Obligatoire. Nom du correctif.
-PatchDescription -ptd	patch_description	Description du correctif.

Option	Argument	Description
-Application -a	application_name	Requis. Nom de l'application incrémentielle pour la mise à jour de laquelle le correctif sera utilisé.
-FilePath -fp	DIS_file_path	Facultatif. Chemin du fichier d'archive de correctif d'application sur la machine du service d'intégration de données. Vous pouvez spécifier un chemin absolu ou relatif vers le fichier.
- OperatingSystemProfile -osp	OSProfile_name	Facultatif. Nom du profil de système d'exploitation. Le nom du profil de système d'exploitation peut comporter jusqu'à 80 caractères. Il ne peut pas inclure d'espaces ou les caractères spéciaux suivants : % * + \ / ? ; < >
- OverwriteDeployedFile -ow	True False	Facultatif. Définissez cette option sur true pour écraser un fichier d'exportation existant. Si un fichier d'exportation existe et que cette option est définie sur false, l'exportation échoue. La valeur par défaut est False.
- MappingDeploymentProperties -mdp	Mapping_Deployment_Property_key=value_pairs_separated_by_semicolon	Facultatif. Définissez les propriétés de déploiement pour le mappage, telles que le niveau d'optimisation, la précision élevée et l'ordre de tri.

DeployApplication

Déploie une application dans un service d'intégration de données.

La commande infacmd dis DeployApplication utilise la syntaxe suivante :

```
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

Le tableau suivant décrit les options et arguments d'infacmd dis DeployApplication :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel est déployée l'application.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
Nom du fichier -f	file_name	Requis. Nom du fichier d'application.
-Application -a	application	Requis. Nom de l'application à déployer. S'il existe un conflit de nom, le déploiement échoue.

disableMappingValidationEnvironment

Désactive l'environnement sélectionné de validation de mappages déployés dans le service d'intégration de données.

Utilisez le paramètre ValidationEnvironment pour désactiver un environnement de validation pour un mappage. Répétez la commande pour chaque environnement à supprimer.

Utilisez les filtres pour spécifier un ou plusieurs mappages dans une application. Si vous n'incluez pas de filtres, la commande met à jour tous les mappages déployés vers le service d'intégration de données. Un mappage doit correspondre à tous les filtres spécifiés pour être modifié.

Les modifications prennent effet une fois que vous recyclez le service d'intégration de données.

La commande infacmd dis disableMappingValidationEnvironment utilise la syntaxe suivante :

```
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]
<-ValidationEnvironment|-ve> validation_environment_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

Le tableau suivant décrit les options et les arguments de la commande disableMappingValidationEnvironment :

Option	Argument	Description
DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
ServiceName -sn	service_name	Requis. Nom du service d'intégration de données.
Application -a	application_name	Facultatif. Nom de l'application qui contient un ou plusieurs mappages. Si vous ne spécifiez pas d'application, la commande met à jour toutes les applications déployées sur le service d'intégration de données.

Option	Argument	Description
-ProjectName -pn	project_name	Facultatif. Nom du projet qui contient le mappage. Si vous ne spécifiez pas de nom de projet, la commande met à jour tous les projets dans le référentiel modèle.
MappingNamesFilter -mnf	noms de mappages	Facultatif. Noms des mappages pour lesquels vous voulez désactiver l'environnement de validation. Séparez les noms de mappage par des virgules. Par défaut, tous les mappages sont déployés vers le service d'intégration de données.
ExecutionEnvironmentFilter -eef	execution_environment_name	Facultatif. Spécifiez l'environnement d'exécution de l'environnement de validation à supprimer. Vous pouvez entrer Natif, Hadoop ou Databricks. Par défaut, l'environnement de validation est modifié pour tous les moteurs en fonction d'autres critères de filtre.
ValidationEnvironment -ve	validation_environment_name	Requis. Nom de l'environnement de validation à supprimer d'un mappage. Vous pouvez entrer l'une des valeurs suivantes : <ul style="list-style-type: none"> - natif - blaze - spark - spark-databricks Exécutez la commande pour chaque environnement de validation à supprimer.
ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

enableMappingValidationEnvironment

Active un environnement de validation pour les mappages déployés sur le service d'intégration de données. Les propriétés d'environnement de validation de mappage indiquent les moteurs dans lesquels le mappage sera validé pour être exécuté.

Utilisez le paramètre `ValidationEnvironment` pour spécifier un environnement de validation. Répétez la commande et spécifiez un environnement de validation différent pour activer un environnement de validation supplémentaire pour le mappage.

Utilisez les filtres pour spécifier un ou plusieurs mappages dans une application ou dans toutes les applications déployées sur un service d'intégration de données. Si vous n'incluez pas de filtres, la commande met à jour tous les mappages déployés vers le service d'intégration de données. Un mappage doit correspondre à tous les filtres spécifiés pour être modifié.

Les modifications prennent effet une fois que vous recyclez le service d'intégration de données.

La commande `infacmd dis enableMappingValidationEnvironment` utilise la syntaxe suivante :

```
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]
<-ValidationEnvironment|-ve> validation_environment_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

Le tableau suivant décrit les options et les arguments de la commande `enableMappingValidationEnvironment` :

Option	Argument	Description
DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
ServiceName -sn	service_name	Requis. Nom du service d'intégration de données.
Application -a	application_name	Facultatif. Nom de l'application qui contient un ou plusieurs mappages. Si vous ne spécifiez pas d'application, la commande met à jour toutes les applications déployées sur le service d'intégration de données.
-ProjectName -pn	project_name	Facultatif. Nom du projet qui contient le mappage. Si vous ne spécifiez pas de nom de projet, la commande met à jour tous les projets dans le référentiel modèle.
ConnectionName -cn	connection_name	Nom de la connexion de l'environnement de validation de mappage à utiliser. La connexion remplace un paramètre de connexion existant ou un paramètre de connexion qui a été défini pour l'environnement. Requise pour activer l'environnement non natif si aucune connexion n'est présente dans le mappage spécifié. Facultatif pour activer l'environnement natif ou si une connexion est déjà présente.
MappingNamesFilter -mnf	noms de mappages	Facultatif. Noms des mappages pour lesquels vous voulez activer l'environnement de validation. Séparez les noms de mappage par des virgules. Par défaut, tous les mappages sont déployés vers le service d'intégration de données.
ExecutionEnvironmentFilter -eef	execution_environment_name	Facultatif. Identifiez l'environnement d'exécution sur lequel filtrer. Vous pouvez entrer Natif, Hadoop ou Databricks. Par défaut, l'environnement de validation est modifié pour tous les moteurs en fonction d'autres critères de filtre.

Option	Argument	Description
ValidationEnvironment -ve	validation_environment_name	Requis. Nom de l'environnement de validation à activer sur un mappage. Vous pouvez entrer l'une des valeurs suivantes : - natif - blaze - spark - spark-databricks Exécutez la commande pour chaque environnement de validation à activer.
ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

ListApplicationObjectPermissions

Répertorie les autorisations d'un utilisateur ou d'un groupe pour un objet d'application comme le mappage ou le flux de travail.

La syntaxe de la commande infacmd dis ListApplicationObjectPermissions est la suivante :

```
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>
```

Le tableau suivant décrit les options et les arguments de la commande infacmd dis
ListApplicationObjectPermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-Application -a	application_name	Requis. Nom de l'application.
-ApplicationObjectType -t	application_object_type	Requis. Type d'objet de l'application. Entrez l'une des valeurs suivantes : - Mappage - Flux de travail
-ApplicationObject -ao	application_object_name	Requis. Nom de l'objet d'application.
-Direct -Effective	direct effective	Requis. Niveau des autorisations à répertorier. Les autorisations directes sont des autorisations attribuées directement à l'utilisateur ou au groupe. Les autorisations effectives comprennent les autorisations directes et les autorisations héritées.

ListApplicationObjects

Répertorie les objets qu'une application contient.

Lorsque vous utilisez l'option -ListObjectTypes, la commande répertorie également le type de chaque objet.

La commande infacmd dis ListApplicationObjects utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd dis ListApplicationObjects :

Option	Argument	Description
-DomainName -dn	domain_name	Facultatif. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-DomainAddress -da	domain_address	Facultatif. Adresse du domaine Informatica.

Option	Argument	Description
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel est déployée l'application.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application	Requis. Nom de l'application.
-ObjectType -t	object_type	Facultatif. Type d'objet à répertorier. Vous pouvez utiliser cette option pour filtrer les résultats par type d'objet.

Option	Argument	Description
-ListObjectType -lt	true false	Facultatif. Entrez l'une des valeurs suivantes : - True - False
-PageSize -ps	page_size	Requis lorsque vous spécifiez l'option PageIndex. Nombre de résultats à afficher dans chaque groupe. Lorsque vous spécifiez une taille de page, vous organisez les résultats de commande dans des groupes. Par exemple, si vous spécifiez -PageSize 5, la commande renvoie les résultats dans des groupes de cinq ou moins.
-PageIndex -pi	page_index	Facultatif. Nombre de résultats par page à afficher à partir de zéro. Par exemple, si vous spécifiez -PageSize 5 -PageIndex 0, la commande renvoie la première page de cinq résultats, de 1 à 5. Si vous ignorez cette option, la commande renvoie la première PageSize de résultats. La valeur par défaut est 0.

ListApplicationOptions

Répertorie les propriétés pour une application.

La commande infacmd dis ListApplicationOptions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd dis ListApplicationOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données dans lequel est déployée l'application.

Option	Argument	Description
-UserName -un	user_name	<p>Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>
-Password -pd	mot de passe	<p>Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p>
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>
-Application -a	application	Obligatoire. Nom de l'application.

ListApplicationPermissions

Répertorie les autorisations que possède un utilisateur ou un groupe pour une application.

La syntaxe de la commande infacmd dis ListApplicationPermissions est la suivante :

```
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>
```

Le tableau suivant décrit les options et les arguments de la commande infacmd dis ListApplicationPermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application_name	Requis. Nom de l'application.
-Direct -Effective	direct effective	Requis. Niveau des autorisations à répertorier. Les autorisations directes sont des autorisations attribuées directement à l'utilisateur ou au groupe. Les autorisations effectives comprennent les autorisations directes et les autorisations héritées.

ListApplications

Répertorie les applications qui sont déployées vers un service d'intégration de données.

La commande infacmd dis ListApplications utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd des ListApplications :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données dont les applications sont à lister.

ListComputeOptions

Répertorie les propriétés du service d'intégration de données pour un nœud doté du rôle de calcul.

La commande infacmd dis ListComputeOptions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande infacmd dis ListComputeOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
NodeName -nn	node_name	Requis. Nœud doté du rôle de calcul qui est attribué au service d'intégration de données ou à la grille du service d'intégration de données.

ListDataObjectOptions

Répertorie les propriétés d'un objet de données.

La commande infacmd dis ListDataObjectOptions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd dis ListDataObjectOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-Application -a	application	Obligatoire. Nom de l'application.
-Folder -f	dossier	Obligatoire. Dossier du service d'archives contenant l'objet de données.
DataObject -do	data_model.data_object	Obligatoire. Nom de l'objet de données.

ListMappingEngines

Répertorie les moteurs d'exécution des mappages déployés dans un service d'intégration de données. Vous pouvez filtrer les résultats en fonction des paramètres de l'application, de l'environnement de validation, de l'environnement d'exécution et de l'environnement d'exécution. Si vous ne spécifiez aucun filtre, la commande répertorie les moteurs d'exécution de tous les mappages déployés.

La syntaxe de la commande `infacmd` `dis listMappingEngines` est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments d'infacmd dis listMappingEngines :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ProjectName -pn	project_name	Facultatif. Nom du projet qui contient le mappage. Si vous ne spécifiez pas de nom de projet, la commande met à jour tous les projets dans le référentiel modèle.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>
Application -a	application_name	<p>Facultatif. Filtre les mappages par l'application déployée qui contient les mappages. Entrez le nom de l'application déployée.</p>
ValidationEnvironmentFilter -vef	validation_environment_name	<p>Facultatif. Filtre les mappages par l'environnement de validation où la définition de mappage est validée. Vous pouvez entrer l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> - natif - blaze - spark - spark-databricks

Option	Argument	Description
ExecutionEnvironmentFilter -eef	execution_environment_name	Facultatif. Filtre les mappages par l'environnement d'exécution où les mappages s'exécutent. Vous pouvez entrer Natif, Hadoop ou Databricks.
ExecutionEnvironmentParamNameFilter -pnf	execution_environment_parameter_name	Facultatif. Filtre les mappages par le paramètre d'environnement d'exécution. Entrez le nom du paramètre d'environnement d'exécution.

ListParameterSetEntries

Répertorie les entrées dans un ensemble de paramètres.

La commande infacmd dis ListParameterSetEntries utilise la syntaxe suivante :

```
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.
```

Le tableau suivant décrit les options et les arguments de la commande infacmd dis ListParameterSetEntries :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel est déployée l'application.

Option	Argument	Description
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application	Requis. Nom de l'application qui contient l'ensemble de paramètres.
parametersetname -ps	nom de l'ensemble de paramètres	Requis. Nom de l'ensemble de paramètres.
-projectScope -prs	portée du projet	Requis. Chemin du mappage ou du flux de travail qui contient les paramètres. Pour un mappage M1 dans un projet P1 et un dossier F1, le chemin est P1/F1/mapping/M1.

ListParameterSetObjects

Répertorie les objets d'un ensemble de paramètres spécifique.

La commande infacmd dis ListParameterSetObjects utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande infacmd dis ListParameterSetObjects :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel est déployée l'application.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-parameterset -ps	ensemble de paramètres	Requis. Nom de l'ensemble de paramètres que vous voulez afficher.
-Application -a	application	Requis. Nom de l'application qui contient l'ensemble de paramètres.

ListParameterSets

Répertorie les ensembles de paramètres dans une application.

La commande infacmd dis ListParameterSets utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande infacmd dis ListParameterSets :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel est déployée l'application.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application	Requis. Nom de l'application qui contient les ensembles de paramètres.

listPatchNames

Répertorie tous les correctifs appliqués à une application incrémentielle.

La syntaxe de la commande infacmd dis listPatchNames est la suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande infacmd dis listPatchNames :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -dun ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -dun est prioritaire.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -dpd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -dsdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.
ResilientTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec ces deux méthodes, l'option -re est prioritaire.
Application -a	application_name	Requis. Nom de l'application incrémentielle.

ListSequenceObjectProperties

Répertorie les propriétés d'un objet de données de séquence.

La commande infacmd dis listsequenceobjectproperties utilise la syntaxe suivante :

```
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
```


Le tableau suivant décrit les options et les arguments de la commande infacmd dis
ListSequenceObjectProperties :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 230 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application	Obligatoire. Nom de l'application.
-SequenceObjectPath -sop	chemin de l'objet de séquence	Obligatoire. Chemin d'accès à l'objet de données de séquence. Le chemin doit inclure les objets suivants dans l'ordre et, le cas échéant : <ul style="list-style-type: none"> - Projet - Dossiers - Service de données SQL ou service Web - Mappage - Transformation Générateur de séquence - Objet de données de séquence Si l'objet de données de séquence se trouve dans un mappage, un service de données SQL ou un service Web, vous devez utiliser un préfixe avant le nom du mappage ou des services. Utilisez les préfixes suivants avec les options dans la commande : <ul style="list-style-type: none"> - Mapping:<nom du mappage> - SQLDS:<nom du service de données SQL> - WS:<nom du service Web> Séparez les options par une barre oblique (/). Par exemple : <nom du projet>/<dossier>/SQLDS:<nom du service de données SQL>/Mapping:<mappage de table virtuelle>/<transformation Générateur de séquence>/<nom de l'objet de données de séquence>

ListSequenceObjects

Répertorie les objets de données de séquence déployés dans une application.

La commande infacmd dis ListSequenceObjects utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd` des `ListSequenceObjects` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 230 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application	Obligatoire. Nom de l'application.

ListServiceOptions

Répertorie les propriétés d'un processus d'intégration des données.

La commande infacmd dis ListServiceOptions utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd dis ListServiceOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données.

Option	Argument	Description
-UserName -un	user_name	<p>Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>
-Password -pd	mot de passe	<p>Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p>
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>

ListServiceProcessOptions

Répertorie les propriétés d'un processus de service d'intégration de données.

La commande infacmd dis ListServiceProcessOptions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd dis ListServiceProcessOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-NodeName -nn	node_name	Obligatoire. Nom de nœud où le processus de service s'exécute.

PurgeDataObjectCache

Purge du cache pour un objet de données logique. Si la mise en cache pour les objets de données logiques est activée, cette commande supprime tous les caches pour un objet de données logique sauf la dernière exécution du cache. Si la dernière exécution du cache est plus vieille que le temps défini dans la propriété Période d'actualisation du cache, la dernière exécution du cache est également supprimée. Si la mise en cache des objets de données logiques n'est pas activée, cette commande supprime tous les caches pour un objet de données logique.

Vous devez désactiver l'application pour un objet de données logique avant de purger le cache de l'objet de données.

La commande infacmd dis PurgeDataObjectCache utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd dis PurgeDataObjectCache :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données dans lequel est déployée l'application.
Application -a	application	Nom de l'application qui contient l'objet de données.
Dossier -f	dossier	Nom du dossier qui contient le modèle d'objet de données.
DataObject -do	data_model.data_object	Nom de l'objet de données dont vous devez purger le cache.
-PurgeAll -pa	vrai faux	Facultatif. Supprime tout le cache pour un objet de données logique.

PurgeResultSetCache

Purge les caches de l'ensemble des résultats pour une application. Vous pouvez purger le cache d'une application lorsque vous n'avez pas besoin des caches de l'ensemble des résultats pour le service de données SQL et les services Web dans l'application.

La commande infacmd dis PurgeResultSetCache utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd dis PurgeResultSetCache :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données dans lequel est déployée l'application.
Application -a	application	Nom de l'application pour laquelle vous voulez purger le cache de l'ensemble des résultats.

queryDesignTimeObjects

Interroge les objets de phase de conception d'un référentiel modèle et renvoie une liste des objets.

La syntaxe de la commande infacmd dis queryDesignTimeObjects est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd dis queryDesignTimeObjects :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données.

Option	Argument	Description
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -dsdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.
-RepositoryService -rs	MRS_service_name	Requis. Nom du service de référentiel modèle.
-RepositoryUserName -rsun	MRS_user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -rsun ou la variable d'environnement INFA_REPOSITORY_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -rsun est prioritaire.
-RepositoryPassword -rspd	MRS_password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -rspd ou la variable d'environnement INFA_REPOSITORY_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -rspd est prioritaire.

Option	Argument	Description
-RepositorySecurityDomain -rssdn	MRS_security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -rssdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -rssdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.
-Query -q	query	Requis. Chaîne qui interroge l'objet. Pour plus d'informations, voir "Requêtes" à la page 280
-TimeZone -tz	time_zone	Facultatif. Par défaut, la commande utilise le fuseau horaire de la machine qui exécute le processus du service d'intégration de données. Pour obtenir une liste des fuseaux horaires valides, reportez-vous à la classe java.time.ZoneID.

queryRunTimeObjects

Interroge les objets d'exécution déployés sur un service d'intégration de données et renvoie une liste des objets.

La syntaxe de la commande infacmd dis queryRunTimeObjects est la suivante :

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

Le tableau suivant décrit les options et les arguments de la commande `infacmd dis queryRunTimeObjects` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -dun ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -dun est prioritaire.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -dpd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -dsdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.
-Query -q	query	Requis. Chaîne qui interroge l'objet. Pour plus d'informations, voir "Requêtes" à la page 280

RefreshDataObjectCache

Actualise le cache de l'objet de données.

La commande `infacmd dis RefreshDataObjectCache` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd dis RefreshDataObjectCache :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données dont vous voulez lister les applications.
-Application -a	application	Obligatoire. Nom de l'application qui contient l'objet de données.
-Folder -f	dossier	Obligatoire. Nom du dossier qui contient l'objet de données.
-DataObject -do	data_model.data_object	Obligatoire. Nom de l'objet de données dont le cache est à actualiser.

RenameApplication

Renomme une application déployée. Avant de renommer une application, exécutez la commande infacmd dis StopApplication pour l'arrêter.

La commande infacmd dis RenameApplication utilise la syntaxe suivante :

```

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

```


Le tableau suivant décrit les options et arguments d'infacmd dis RenameApplication :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données dans lequel l'application est déployée.

Option	Argument	Description
-Application -a	application	Obligatoire. Nom de l'application actuelle.
-NewName -n	new_name	Obligatoire. Nouveau nom pour l'application.

replaceMappingHadoopRuntimeConnections

Remplace la connexion Hadoop de tous les mappages dans les applications déployées par une autre connexion Hadoop. Le Service d'intégration de données utilise la connexion Hadoop pour se connecter au cluster Hadoop pour exécuter des mappages dans l'environnement Hadoop.

La commande ne modifie pas les connexions Hadoop dans les transformations. Vous pouvez spécifier le nom de l'application pour remplacer la connexion Hadoop d'une application.

La commande infacmd dis replaceMappingHadoopRuntimeConnections utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande replaceMappingHadoopRuntimeConnections :

Option	Argument	Description
DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
ServiceName -sn	service_name	Requis. Nom du service d'intégration de données.

Option	Argument	Description
UserName -un	user_name	<p>Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>
Password -pd	mot de passe	<p>Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p>
SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>

Option	Argument	Description
ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
ApplicationName -an	application_name	Facultatif. Nom de l'application qui contient le mappage. Si vous spécifiez cette option, la commande remplace la connexion Hadoop uniquement pour l'application.
OldConnectionName -oc	connection_name_of_old_connection_to_replace	Requis. Nom de la connexion Hadoop à remplacer.
NewConnectionName -nc	connection_name_of_new_connection	Requis. Nom de la connexion Hadoop que le service d'intégration de données doit utiliser pour se connecter à la grappe Hadoop afin d'exécuter des mappages dans l'environnement Hadoop.

RestoreApplication

Restaure une application à partir d'un fichier de sauvegarde. Lorsque vous déployez une application restaurée, l'état de l'application dépend du mode de déploiement par défaut. Les propriétés de l'application sont conservées dans l'application restaurée.

La commande infacmd dis RestoreApplication utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd dis RestoreApplication :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données auquel restaurer l'application.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-FileName -f	file_name	Obligatoire. Nom du fichier de sauvegarde de l'application.
-Application -a	application	Facultatif. Nom de l'application après l'avoir déployée. S'il existe un conflit de nom, le déploiement échoue.

SetApplicationPermissions

Attribue ou refuse les autorisations sur une application à un utilisateur ou à un groupe.

Vous pouvez autoriser les utilisateurs ou refuser l'autorisation à l'aide des options -ap ou -dp de la commande SetApplicationPermissions. Si vous n'autorisez pas les utilisateurs ou ne refusez pas l'autorisation explicitement à l'aide de l'une des options, toutes les autorisations sur l'application sont révoquées.

La syntaxe de la commande infacmd dis SetApplicationPermissions est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd dis SetApplicationPermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.

Option	Argument	Description
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application_name	Requis. Nom de l'application.
-GranteeUserName GranteeGroupName -gun -ggn	grantee_user_name grantee_group_name	Requis. Nom d'utilisateur ou nom de groupe pour lequel définir ou refuser des autorisations.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Requis si vous utilisez une authentification LDAP et que vous attribuez des autorisations d'utilisateur. Nom du domaine de sécurité auquel appartient l'utilisateur.

Option	Argument	Description
-AllowedPermissions -ap	allowed_permissions	Facultatif. Liste des autorisations à accepter. Entrez les autorisations suivantes séparées par des espaces : <ul style="list-style-type: none"> - Afficher. Les utilisateurs peuvent afficher l'application. - Grant. Les utilisateurs peuvent accorder et retirer des autorisations sur l'application. - Execute. Les utilisateurs peuvent exécuter l'application.
-DeniedPermissions -dp	denied_permissions	Facultatif. Liste des autorisations pour refuser des utilisateurs. Séparez chaque paramètre par une espace. Entrez les autorisations suivantes séparées par des espaces : <ul style="list-style-type: none"> - Afficher. Les utilisateurs peuvent afficher l'application. - Grant. Les utilisateurs ne peuvent pas accorder ou retirer des autorisations sur l'application. - Execute. Les utilisateurs ne peuvent pas exécuter l'application.

SetApplicationObjectPermissions

Attribue ou refuse les autorisations sur un objet d'application, tel qu'un mappage ou un flux de travail à un utilisateur ou à un groupe.

Vous pouvez autoriser les utilisateurs ou refuser l'autorisation à l'aide des options -ap ou -dp de la commande SetApplicationObjectPermissions. Si vous n'autorisez pas les utilisateurs ou ne refusez pas l'autorisation explicitement à l'aide de l'une des options, les utilisateurs héritent des autorisations de niveau application sur le mappage ou le flux de travail.

La syntaxe de la commande infacmd dis SetApplicationObjectPermissions est la suivante :

```
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]
```


Le tableau suivant décrit les options et les arguments de la commande `infacmd dis SetApplicationObjectPermissions` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-Application -a	application_name	Requis. Nom de l'application.
-ApplicationObjectType -t	application_object_type	Requis. Type d'objet de l'application. Entrez l'une des valeurs suivantes : - Mappage - Flux de travail
-ApplicationObject -ao	application_object_name	Requis. Nom de l'objet d'application.
-GranteeUserName GranteeGroupName -gun -ggn	grantee_user_name grantee_group_name	Requis. Nom d'utilisateur ou nom de groupe pour lequel définir ou refuser des autorisations.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Requis si vous utilisez une authentification LDAP et que vous attribuez des autorisations d'utilisateur. Nom du domaine de sécurité auquel appartient l'utilisateur.
-AllowedPermissions -ap	allowed_permissions	Facultatif. Liste des autorisations à accepter. Entrez les autorisations suivantes séparées par des espaces : - Afficher. Les utilisateurs peuvent afficher l'application. - Grant. Les utilisateurs peuvent accorder et retirer des autorisations sur l'application. - Execute. Les utilisateurs peuvent exécuter l'application.
-DeniedPermissions -dp	denied_permissions	Facultatif. Liste des autorisations pour refuser des utilisateurs. Séparez chaque paramètre par une espace. Entrez les autorisations suivantes séparées par des espaces : - Afficher. Les utilisateurs peuvent afficher l'application. - Grant. Les utilisateurs ne peuvent pas accorder ou retirer des autorisations sur l'application. - Execute. Les utilisateurs ne peuvent pas exécuter l'application.

setMappingExecutionEnvironment

Spécifie l'environnement d'exécution des mappages déployés sur le service d'intégration de données.

Utilisez des filtres pour spécifier une liste de mappages, tous les mappages dans une application ou toutes les applications déployées dans un service d'intégration de données. Si vous n'incluez pas de filtres, la commande met à jour tous les mappages déployés vers le service d'intégration de données. Un mappage doit correspondre à tous les filtres spécifiés pour être modifié.

Les modifications prennent effet une fois que vous recyclez le service d'intégration de données.

La commande infacmd dis setMappingExecutionEnvironment utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et les arguments de la commande setMappingExecutionEnvironment :

Option	Argument	Description
DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-ProjectName -pn	project_name	Facultatif. Nom du projet qui contient le mappage. Si vous ne spécifiez pas de nom de projet, la commande met à jour tous les projets dans le référentiel modèle.
MappingNamesFilter -mnf	noms de mappages	Facultatif. Noms des mappages pour lesquels vous souhaitez définir l'environnement d'exécution. Séparez les noms de mappage par des virgules. Par défaut, tous les mappages sont déployés vers le service d'intégration de données.
ExecutionEnvironment -ee	execution_environment_name	Requis. Identifiez l'environnement d'exécution à définir. Choisissez Natif, Hadoop ou Databricks.
ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
NewConnectionName -nc	connection_name_of_new_connection	Obligatoire. Nom de la connexion Hadoop ou Databricks que le service d'intégration de données doit utiliser pour se connecter au cluster de calcul afin d'exécuter des mappages dans l'environnement non natif.

SetSequenceState

Met à jour la valeur actuelle d'un objet de données de séquence.

La commande infacmd dis SetSequenceState utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande infacmd dis SetSequenceState :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 230 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIANCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application	Obligatoire. Nom de l'application.
-SequenceObjectPath -sop	chemin de l'objet de séquence	<p>Obligatoire. Chemin d'accès à l'objet de données de séquence. Le chemin peut inclure les objets suivants dans l'ordre et s'il y a lieu :</p> <ul style="list-style-type: none"> - Projet - Dossiers - Service de données SQL ou service Web - Mappage - Transformation Générateur de séquence - Objet de données de séquence <p>Pour mettre à jour un objet de données de séquence réutilisable, spécifiez le chemin en utilisant uniquement le projet, les dossiers et l'objet de données séquence.</p> <p>Pour mettre à jour un objet de données de séquence non réutilisable qui se trouve dans un service de données SQL ou un service Web, utilisez un préfixe avant le nom du service de données SQL ou du service Web. Utilisez les préfixes suivants avec les options dans la commande :</p> <ul style="list-style-type: none"> - SQLEP:<nom du service de données SQL> - WSEP:<nom du service Web> <p>Séparez les options par une barre oblique (/). Par exemple :</p> <pre><project name>/<folder name>/WSEP:<web service name>/<operation mapping name>/<Sequence Generator transformation name>/<sequence data object name></pre>
-SequenceValue -sv	sequence_value	Obligatoire. Nouvelle valeur de l'objet de données de séquence. Entrez une valeur supérieure ou égale à la valeur de départ de l'objet de données de séquence et inférieure ou égale à la valeur finale.

StartApplication

Démarre une application déployée. Vous devez activer l'application avant de pouvoir la démarrer. Le service d'intégration des données est en cours d'exécution.

La commande infacmd dis StartApplication utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd dis StartApplication :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données dans lequel est déployée l'application.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application	Obligatoire. Nom de l'application à démarrer.

StopApplication

Interrompt l'exécution d'une application. Vous pouvez arrêter une application si vous devez la sauvegarder ou si vous voulez empêcher les utilisateurs d'y accéder.

La commande infacmd dis StopApplication utilise la syntaxe suivante :

```
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
```


Le tableau suivant décrit les options et arguments d'infacmd dis StopApplication :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données dans lequel l'application est déployée.
-Application -a	application	Obligatoire. Nom de l'application à arrêter.

stopBlazeService

Arrête l'exécution des composants du moteur Blaze. Vous pouvez arrêter l'exécution des composants du moteur Blaze afin d'effectuer la maintenance de la grappe Hadoop, comme le nettoyage des ressources ou l'application de correctifs logiciels.

La syntaxe de la commande infacmd dis stopBlazeService est la suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd dis stopBlazeService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données dans lequel l'application est déployée.

Option	Argument	Description
-UserName -un	user_name	<p>Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>
-Password -pd	password	<p>Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p>

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-HadoopConnection -hc	Hadoop_Cluster_Connection_Name	Obligatoire. Nom de la connexion Hadoop que le service d'intégration de données utilise pour exécuter le mappage sur le moteur Blaze.

Remarque: Lorsque vous exécutez la commande stopBlazeService, certains journaux de composants peuvent ne pas être consignés dans les fichiers journaux agrégés sur HDFS. Vous pouvez afficher les journaux dans

le répertoire configuré pour les journaux du moteur Blaze en fonction de la propriété avancée suivante de Blaze dans la connexion Hadoop : `infagrid.node.local.root.log.dir`

tag

Attribuez des balises à des objets de phase de conception.

Les balises sont des métadonnées qui définissent un objet dans le service de référentiel modèle. Interrogez les objets et spécifiez des balises pour grouper les objets selon leur utilisation métier. Si vous réattribuez une balise à un objet, la commande remplacera la balise existante.

La syntaxe de la commande `infacmd dis tag` est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd dis tag` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	DIS_service_name	Requis. Nom du service d'intégration de données.

Option	Argument	Description
-UserName -un	DIS_user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Password -pd	DIS_password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	DIS_security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.
RepositoryService -rs	MRS_service_name	Requis. Nom du service de référentiel modèle.
-RepositoryUserName -rsun	MRS_user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -rsun ou la variable d'environnement INFA_REPOSITORY_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -rsun est prioritaire.
-RepositoryPassword -rspd	MRS_password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -rspd ou la variable d'environnement INFA_REPOSITORY_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -rspd est prioritaire.

Option	Argument	Description
RepositorySecurityDomain -rssdn	MRS_security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -rssdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -rssdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.
-Query -q	Query	Requis. Chaîne qui interroge le référentiel à la recherche d'un nom de balise. Pour plus d'informations, voir "Requêtes" à la page 280 .
-TagName -tn	tag_name	Obligatoire. Nom de la balise que vous souhaitez attribuer à l'objet interrogé. Le nom ne doit pas dépasser 128 caractères ni commencer par un nombre. Le nom doit comporter des caractères alphanumériques. Vous pouvez également utiliser les caractères spéciaux tels que @ # _.
-TagDescription -td	tag_description	Facultatif. Description de la balise.
-TimeZone -tz	time_zone	Facultatif. Par défaut, la commande utilise le fuseau horaire de la machine qui exécute le processus du service d'intégration de données. Pour obtenir une liste des fuseaux horaire valides, reportez-vous à la classe java.time.ZoneID.

untag

Supprime les balises des objets de phase de conception.

Si l'utilisation métier a changé, supprimez les balises pour dégroupier les objets. Interrogez les objets et spécifiez les balises à supprimer.

La syntaxe de la commande infacmd dis untag est la suivante :

```
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]

```

Le tableau suivant décrit les options et les arguments de la commande infacmd dis untag :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	DIS_service_name	Requis. Nom du service d'intégration de données.
-UserName -un	DIS_user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Password -pd	DIS_password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	DIS_security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.
-RepositoryService -rs	MRS_service_name	Requis. Nom du service de référentiel modèle.
-RepositoryUserName -rsun	MRS_user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -rsun ou la variable d'environnement INFA_REPOSITORY_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -rsun est prioritaire.
-RepositoryPassword -rspd	MRS_password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -rspd ou la variable d'environnement INFA_REPOSITORY_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -rspd est prioritaire.

Option	Argument	Description
-RepositorySecurityDomain -rssdn	MRS_security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -rssdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -rssdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.
-Query -q	Query	Requis. Chaîne qui interroge le référentiel à la recherche d'un nom de balise. Pour plus d'informations, voir "Requêtes" à la page 280
-TagName -tn	tag_name	Obligatoire. Nom de la balise que vous souhaitez supprimer de l'objet interrogé.
-TimeZone -tz	time_zone	Facultatif. Par défaut, la commande utilise le fuseau horaire de la machine qui exécute le processus du service d'intégration de données. Pour obtenir une liste des fuseaux horaire valides, reportez-vous à la classe java.time.ZoneID.

replaceAllTag

Remplace toutes les balises attribuées aux objets de phase de conception.

Interrogez les objets et remplacez les balises attribuées. Si l'utilisation métier a changé, vous pouvez utiliser la commande pour dégroupier les objets et attribuer de nouvelles balises pour les regrouper. Toutes les balises attribuées sont supprimées et remplacées par la balise spécifiée.

La syntaxe de la commande infacmd dis replaceAllTag est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd dis replaceAllTag :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	DIS_service_name	Requis. Nom du service d'intégration de données.
-UserName -un	DIS_user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Password -pd	DIS_password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	DIS_security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.

Option	Argument	Description
-RepositoryService -rs	MRS_service_name	Requis. Nom du service de référentiel modèle.
-RepositoryUserName -rsun	MRS_user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -rsun ou la variable d'environnement INFA_REPOSITORY_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -rsun est prioritaire.
-RepositoryPassword -rspd	MRS_password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -rspd ou la variable d'environnement INFA_REPOSITORY_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -rspd est prioritaire.
-RepositorySecurityDomain -rssdn	MRS_security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -rssdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -rssdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native.
-Query -q	query	Requis. Chaîne qui interroge le référentiel à la recherche d'un nom de balise. Pour plus d'informations, voir "Requêtes" à la page 280
-TagName -tn	tag_name	Obligatoire. Nom de la balise de remplacement que vous souhaitez attribuer aux objets interrogés. Le nom ne doit pas dépasser 128 caractères ni commencer par un nombre. Le nom doit comporter des caractères alphanumériques. Vous pouvez également utiliser les caractères spéciaux tels que @ # _.

Option	Argument	Description
-TagDescription -td	tag_description	Facultatif. Description de la balise.
-TimeZone -tz	time_zone	Facultatif. Par défaut, la commande utilise le fuseau horaire de la machine qui exécute le processus du service d'intégration de données. Pour obtenir une liste des fuseaux horaire valides, reportez-vous à la classe java.time.ZoneID.

UndeployApplication

Supprime une application d'un service d'intégration de données.

La commande infacmd dis UndeployApplication utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd dis UndeployApplication :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom du domaine avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données d'où doit être retirée l'application.
-Application -a	application	Obligatoire. Nom de l'application à retirer du service d'intégration de données.

UpdateApplication

Met à jour une application à partir d'un fichier d'application et conserve la configuration. L'application doit être déployée vers un service d'intégration des données. Les utilisateurs finaux peuvent accéder à la dernière version de l'application.

La commande infacmd dis UpdateApplication utilise la syntaxe suivante :

```
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]

```

Le tableau suivant décrit les options et arguments d'infacmd dis UpdateApplication :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données dans lequel l'application est déployée.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-FileName -f	file_name	Obligatoire. Nom et chemin du fichier application pour la mise à jour de l'application déployée.
-Application -a	application	Facultatif. Nom de l'application déployée.

UpdateApplicationOptions

Met à jour les propriétés de l'application.

Séparez chaque option et valeur par un espace. Pour afficher les propriétés actuelles, exécutez la commande infacmd dis ListApplicationOptions.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Séparez les options multiples par un espace. Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

La commande infacmd dis UpdateApplicationOptions utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et arguments de la commande `infacmd` dis `UpdateApplicationOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données dans lequel est déployée l'application.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application	Obligatoire. Nom de l'application à mettre à jour.
-Options -o	options	Obligatoire. Entrez chaque option et valeur à mettre à jour. Séparez chaque option par un espace. Pour afficher les options de l'application, exécutez la commande infacmd dis ListApplicationOptions.

UpdateComputeOptions

Met à jour les propriétés du service d'intégration de données pour un nœud ayant un rôle de calcul. Utilisez la commande pour remplacer les propriétés du service d'intégration de données pour un nœud de calcul spécifique.

Entrez les options en utilisant le format suivant :

```
... -o option_name=value option_name=value ...
```

Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

La commande infacmd dis UpdateComputeOptions utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et les arguments de la commande infacmd dis UpdateComputeOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
NodeName -nn	node_name	Requis. Nœud doté du rôle de calcul qui est attribué au service d'intégration de données ou à la grille du service d'intégration de données.
-Options -o	options	Requis. Entrez chaque option en la séparant par un espace. Pour afficher les options, exécutez la commande infacmd dis ListComputeOptions. Vous pouvez mettre à jour les options suivantes du service d'intégration de données : <ul style="list-style-type: none"> - ExecutionOptions.TemporaryDirectories - ExecutionOptions.DISHomeDirectory - ExecutionOptions.CacheDirectory - ExecutionOptions.SourceDirectory - ExecutionOptions.TargetDirectory - ExecutionOptions.RejectFilesDirectory

UpdateDataObjectOptions

Met à jour les propriétés de l'objet de données. Pour afficher les options actuelles, exécutez la commande infacmd dis ListDataObjectOptions.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Séparez les options multiples par un espace. Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

La commande infacmd dis UpdateDataObjectOptions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments de la commande infacmd dis UpdateDataObjectOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données dans lequel est déployée l'application.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application	Obligatoire. Application qui contient l'objet de données.
-Folder -f	Dossier	Obligatoire. Nom du dossier qui contient le modèle d'objet de données.
-DataObject -do	data_model.data_object	Obligatoire. Nom de l'objet de données que vous souhaitez mettre à jour.
-Options -o	options	Obligatoire. Entrez les options et les valeurs en les séparant par des espaces. Pour afficher les options actuelles, exécutez la commande infacmd dis ListDataObjectOptions.

Options des objets de données

Utilisez les options des objets de données pour configurer la mise en cache d'un objet de données logique. Utilisez les options des objets de données avec la commande infacmd dis UpdateDataObjectOptions.

Entrez les options des objets de données au format suivant :

```
... -o option_type.option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options des objets de données :

Option	Description
DataObjectOptions.CachingEnabled	Met en cache l'objet de données logique dans la base de données du cache d'objet de données. True ou False. La valeur par défaut est True.
DataObjectOptions.CacheRefreshPeriod	Nombre de minutes entre les actualisations du cache. La valeur par défaut est zéro.
DataObjectOptions.CacheTableName	<p>Nom de la table gérée par l'utilisateur à partir de laquelle le service d'intégration de données accède au cache d'objet de données logique. Une table de cache gérée par l'utilisateur est une table de la base de données du cache d'objet de données que vous créez, remplissez et actualisez manuellement si nécessaire.</p> <p>Si vous spécifiez un nom de table de cache, le gestionnaire de cache d'objet de données ne gère pas le cache de l'objet et ignore la période d'actualisation du cache. Si vous ne spécifiez pas de nom de table de cache, le gestionnaire de cache d'objet de données gère le cache de l'objet.</p>

UpdateParameterSetEntries

Met à jour les entrées à partir d'un ensemble de paramètres. Exécutez cette commande pour mettre à jour les valeurs dans les entrées de l'ensemble de paramètres d'un mappage ou d'un flux de travail dans une application.

La commande infacmd dis UpdateParameterSetEntries utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande infacmd dis UpdateParameterSetEntries :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel est déployée l'application.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-Application -a	application	Requis. Nom de l'application qui contient l'ensemble de paramètres.
parametersetname -ps	nom de l'ensemble de paramètres	Requis. Nom de l'ensemble de paramètres.
-projectScope -prs	portée du projet	Requis. Chemin du mappage ou du flux de travail qui contient les paramètres. Pour un mappage M1 dans un projet P1 et un dossier F1, le chemin est P1/F1/mapping/M1.
-paramNames -pnv	noms de paramètre	Requis. Paramètre des paires nom-valeur séparées par un espace. Placez les paires nom-valeur entre guillemets doubles. Placez chaque valeur entre des guillemets simples. Utilisez la syntaxe suivante : "parm1='valueA'" "parm2='valueB'" "parm3='valueC'" . Vous pouvez inclure des espaces dans une valeur de paramètre. Vous pouvez inclure une apostrophe (') ou un signe deux-points (:) dans la valeur si vous échappez le caractère à l'aide d'une barre oblique inversée (\). 'C:\directory'

UpdateServiceOptions

Met à jour les propriétés du service d'intégration de données. Pour afficher les propriétés actuelles, exécutez la commande `infacmd dis ListServiceOptions`.

Vous pouvez modifier les propriétés du service ainsi que le service à exécuter sur un nœud unique ou dans une grille. Les modifications prennent effet une fois que vous recyclez le service. Vous pouvez utiliser l'option `RecycleMode (-rm)` pour recycler le service.

```
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,...]
```

Le tableau suivant décrit les options et arguments de la commande `infacmd dis UpdateServiceOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-Options -o	options	Facultatif. Entrez chaque option en la séparant par un espace. Pour afficher les options, exécutez la commande <code>infacmd dis ListServiceOptions</code> .
-NodeName -nn	node_name	Pour supprimer le service d'intégration de données d'une grille et l'exécuter sur un nœud unique, entrez le nom du nœud. Vous pouvez entrer le nom du nœud ou le nom de la grille, mais pas les deux à la fois.
-GridName -gn	grid_name	Pour déplacer le service d'intégration de données d'un nœud unique vers une grille, entrez le nom de la grille. Vous pouvez entrer le nom du nœud ou le nom de la grille, mais pas les deux à la fois.
-RecycleMode -rm	recycle_mode	Facultatif. Le mode de recyclage redémarre le service et applique les dernières propriétés du service et du processus de service. Sélectionnez Abandonner ou Terminer. <ul style="list-style-type: none"> - Terminer. Arrête toutes les applications et annule toutes les tâches dans chaque application. Attend que toutes les tâches soient annulées pour désactiver le service. - Abandonner. Arrête toutes les applications et tente d'annuler toutes les tâches avant de les abandonner et de désactiver le service. La valeur par défaut est Terminer.
-BackupNodes -bn	node_name1,node_name2,.. ..	Facultatif. Nœuds sur lesquels le service peut s'exécuter si le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.

Options du service d'intégration de données

Utilisez les options du service d'intégration de données avec la commande `infacmd dis UpdateServiceOptions`.

Entrez les options du service d'intégration de données au format suivant :

```
... -o option_type.option_name=value
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options du service d'intégration de données :

Option	Description
<code>AdvancedProfilingServiceOptions.ColumnsPerMapping</code>	Limite le nombre de colonnes pouvant être profilées en un seul mappage afin d'économiser de la mémoire et de l'espace disque. La valeur par défaut est 5. Si vous profilez une source comportant plus de 100 millions de lignes, réduisez la valeur à 1.
<code>AdvancedProfilingServiceOptions.ExecutionPoolSize</code>	Nombre maximal de threads pour exécuter des mappages.

Option	Description
AdvancedProfilingServiceOptions.MaxMemPerRequest	Quantité maximale de mémoire, en octets, que le service d'intégration de données peut allouer pour chaque exécution de mappage à une seule demande de profil. La valeur par défaut est 536 870 912.
AdvancedProfilingServiceOptions.MaxNumericPrecision	Nombre maximal de chiffres pour une valeur numérique.
AdvancedProfilingServiceOptions.MaxParallelColumnBatches	Nombre de threads pouvant exécuter des mappages en même temps. La valeur par défaut est 1.
AdvancedProfilingServiceOptions.MaxStringLength	Longueur maximale d'une chaîne que le service de profilage peut traiter.
AdvancedProfilingServiceOptions.MaxValueFrequencyPairs	Nombre maximal de paires valeur/fréquence à stocker dans l'entrepôt de profilage. La valeur par défaut est 16 000.
AdvancedProfilingServiceOptions.MinPatternFrequency	Nombre minimal de modèles à afficher pour un profil.
AdvancedProfilingServiceOptions.ReservedThreads	Nombre de threads de la taille de pool d'exécution maximale destinés aux demandes prioritaires. La valeur par défaut est 1.
AdvancedProfilingServiceOptions.ValueFrequencyMemSize	Quantité de mémoire à autoriser pour permettre des paires valeur/fréquence. La valeur par défaut est 64 mégaoctets.
DataObjectCacheOptions.CacheConnection	Nom de connexion de la base de données qui stocke le cache de l'objet de données. Entrez un nom d'objet de connexion valide.
DataObjectCacheOptions.CacheRemovalTime	Nombre de millisecondes pendant lequel le service d'intégration de données attend avant de nettoyer la mémoire cache après une actualisation. La valeur par défaut est 3 600 000.
DeploymentOptions.DefaultDeploymentMode	Détermine s'il convient d'activer et de démarrer chaque application après l'avoir déployée sur un service d'intégration de données. Entrez l'une des options suivantes : <ul style="list-style-type: none"> - EnableandStart. Activer et démarrer l'application. - EnableOnly. Activer l'application, mais sans la démarrer. - Désactiver. Ne pas activer l'application.

Option	Description
DataObjectCacheOptions.EnableNestedLDOCache	<p>Indique que le service d'intégration de données peut utiliser les données de cache pour un objet de données logique utilisé comme source ou recherche dans un autre objet de données logique lors d'une actualisation du cache. Si la valeur est False, le service d'intégration de données accède aux ressources de la source, même si avez activé la mise en cache pour l'objet de données logique utilisé comme source ou recherche.</p> <p>Par exemple, l'objet de données logique LDO3 joint des données des objets de données logiques LDO1 et LDO2. Un développeur crée un mappage qui utilise LDO3 comme entrée et inclut le mappage dans une application. Vous activez la mise en cache pour LDO1, LDO2 et LDO3. Si vous activez la mise en cache d'objets de données logiques imbriqués, le service d'intégration de données utilise les données de cache pour LDO1 et LDO2 lorsqu'il actualise la table de cache pour LDO3. Si vous n'activez pas la mise en cache d'objets de données logiques imbriqués, le service d'intégration de données accède aux ressources de la source pour LDO1 et LDO2 lorsqu'il actualise la table de cache pour LDO3.</p> <p>La valeur par défaut est False.</p>
DataObjectCacheOptions.MaxConcurrentRefreshRequests	<p>Nombre maximal d'actualisations du cache qui peuvent se produire en même temps.</p>
ExecutionContextOptions.Spark.MSPEnableUnassignedData	<p>Si la valeur est True, active la fonctionnalité d'analyse en cours qui capture les données non analysées dans la chaîne source et les enregistre dans un tableau <code>UnassignedData</code> sous forme d'un <code>unidentifiedDataItem</code>.</p> <p>Par défaut, si l'analyseur rencontre un champ de données qu'il ne peut pas analyser, les données sont ignorées. Toutefois, les données complexes de la chaîne source peuvent être modifiées. Par exemple, une mise à jour logicielle sur le serveur peut modifier le fichier JSON ou XML. Cette option permet de capturer les données pour l'analyse.</p> <p>La valeur par défaut est False.</p>
ExecutionOptions.BigDataJobRecovery	<p>Si la valeur est True, active la récupération de la tâche Data Engineering et la mise en file d'attente distribuée pour les tâches déployées configurées pour être exécutées sur le moteur Spark.</p> <p>La valeur par défaut est false.</p>
ExecutionOptions.CacheDirectory	<p>Répertoire des fichiers d'index et de cache de données des transformations. La valeur par défaut est <code><home directory>/cache</code>.</p> <p>Entrez une liste de répertoires séparés par des points-virgules afin d'augmenter les performances pendant le partitionnement du cache des transformations Agrégation, Jointure ou Rang.</p> <p>Vous ne pouvez pas utiliser les caractères suivants dans le chemin du répertoire :</p> <p>* ? < > " ,</p>
ExecutionOptions.DisHadoopKeytab	<p>Chemin du fichier Keytab Kerberos sur la machine sur laquelle le service d'intégration de données s'exécute.</p>

Option	Description
ExecutionOptions.DisHadoopPrincipal	Nom de principal du service (SPN) d'intégration de données permettant de se connecter à une grappe Hadoop qui utilise l'authentification Kerberos.
ExecutionOptions.DISHomeDirectory	<p>Répertoire racine accessible au nœud. Il s'agit du répertoire racine d'autres répertoires de service. La valeur par défaut est <Informatica installation directory>/tomcat/bin. Si vous modifiez la valeur par défaut, vérifiez que le répertoire existe.</p> <p>Vous ne pouvez pas utiliser les caractères suivants dans le chemin du répertoire :</p> <p>* ? < > " ,</p>
ExecutionOptions.EnableOSProfile	Indique que le service d'intégration de données peut utiliser les profils du système d'exploitation pour l'exécution du mappage. Vous pouvez activer les profils du système d'exploitation si le service d'intégration de données est exécuté sur UNIX ou Linux. La valeur par défaut est false.
ExecutionOptions.HadoopDistributionDir	<p>Répertoire contenant un ensemble de fichiers JAR Hadoop sur le cluster des emplacements d'installation du RPM. Le répertoire contient l'ensemble minimal de fichiers JAR requis pour traiter les mappages Informatica dans un environnement Hadoop.</p> <p>Entrez /</p> <p><PowerCenterBigDataEditionInstallationDirectory>/Informatica/services/shared/hadoop/[Hadoop_distribution_name].</p>
ExecutionOptions.HadoopInfraHomeDir	<p>Répertoire de base de PowerCenter Big Data Edition sur chaque nœud de données créé par l'installation du RPM Hadoop.</p> <p>Entrez /</p> <p><PowerCenterBigDataEditionInstallationDirectory>/Informatica.</p>
ExecutionOptions.MaxHadoopBatchExecutionPool Size	Nombre maximal de tâches déployées qui peuvent s'exécuter simultanément dans l'environnement Hadoop. Le service d'intégration de données déplace les tâches Hadoop de la file d'attente vers le pool de tâches Hadoop lorsque des ressources suffisantes sont disponibles. La valeur par défaut est 100.

Option	Description
ExecutionOptions.MaxMappingParallelism	<p>Nombre maximal de threads parallèles qui traitent une seule étape du pipeline du mappage.</p> <p>Lorsque vous définissez la valeur sur un nombre supérieur à un, le service d'intégration de données active le partitionnement pour les mappages et pour les mappages convertis à partir des profils. Le service met à l'échelle de manière dynamique le nombre de partitions pour un pipeline de mappage lors de l'exécution. Augmentez la valeur en fonction du nombre de processeurs disponibles sur les nœuds sur lesquels des mappages s'exécutent.</p> <p>Dans l'outil Developer tool, les développeurs peuvent modifier la valeur de parallélisme maximale pour chaque mappage. Lorsque le parallélisme maximal est défini pour le service d'intégration de données et le mappage, le service d'intégration de données utilise la valeur minimale lorsqu'il exécute le mappage.</p> <p>La valeur par défaut est 1. La valeur maximale est 64.</p>
ExecutionOptions.MaxMemorySize	<p>Quantité maximale de mémoire, en octets, que le service d'intégration de données peut allouer pour l'exécution simultanée de toutes les demandes lorsqu'il exécute les tâches dans le processus de service d'intégration de données. Lorsque le service d'intégration de données exécute les tâches dans des processus locaux ou distants distincts, il ignore cette valeur. Si vous ne voulez pas limiter la quantité de mémoire que le service d'intégration de données peut allouer, définissez cette propriété sur 0.</p> <p>Si la valeur est supérieure à 0, le service d'intégration de données utilise la propriété pour calculer la quantité maximale totale de mémoire autorisée pour l'exécution simultanée de toutes les demandes. Le service d'intégration de données calcule la taille maximale de mémoire comme suit :</p> <p>Taille maximale de la mémoire + Taille maximale du tas mémoire + Mémoire requise pour le chargement des composants de programme</p> <p>La valeur par défaut est 0.</p> <p>Remarque: si vous exécutez des profils ou des mappages de qualité des données, définissez cette propriété sur 0.</p>
ExecutionOptions.MaxNativeBatchExecutionPoolSize	<p>Nombre maximal de tâches déployées qui peuvent s'exécuter simultanément dans l'environnement natif. Le service d'intégration de données déplace les tâches de mappage natives de la file d'attente vers le pool de tâches natif lorsque des ressources suffisantes sont disponibles. La valeur par défaut est 10.</p>
ExecutionOptions.MaxOnDemandExecutionPoolSize	<p>Nombre maximal de tâches à la demande qui peuvent s'exécuter simultanément. Les tâches incluent des aperçus de données, des tâches de profilage, des requêtes REST et SQL, des demandes de service Web et des mappages exécutés à partir de l'outil Developer tool. Toutes les tâches que le service d'intégration de données reçoit contribuent à la taille de pool à la demande. Le service d'intégration de données exécute immédiatement les tâches à la demande si des ressources suffisantes sont disponibles. Sinon, le service d'intégration de données rejette la tâche. La valeur par défaut est 10.</p>

Option	Description
ExecutionOptions.OutOfProcessExecution	<p>Exécute les tâches dans le processus de service d'intégration de données, dans des processus DTM séparés sur le nœud local ou dans des processus DTM séparés sur des nœuds distants. Configurez la propriété selon que le service d'intégration de données s'exécute sur un nœud unique ou sur une grille et en fonction des types de tâches qu'il exécute.</p> <p>Entrez l'une des options suivantes :</p> <ul style="list-style-type: none"> - IN_PROCESS. Exécute les tâches dans le processus de service d'intégration de données. Sélectionnez cette option lorsque vous exécutez les tâches de service de données SQL et de service Web sur un seul nœud ou sur une grille dont les nœuds sont dotés à la fois des rôles de service et de calcul. - OUT_OF_PROCESS. Exécute des tâches dans des processus DTM distincts sur le nœud local. Sélectionnez cette option lorsque vous exécutez les tâches de mappage, de profil et de flux de travail sur un seul nœud ou sur une grille dont les nœuds sont dotés à la fois des rôles de service et de calcul. - OUT_OF_PROCESS_REMOTE. Exécute des tâches dans des processus DTM distincts sur des nœuds distants. Sélectionnez cette option lorsque vous exécutez les tâches de mappage, de profil et de flux de travail sur une grille dont les nœuds peuvent présenter différentes combinaisons de rôles. Si vous sélectionnez cette option lorsque le service d'intégration de données s'exécute sur un seul nœud, le service exécute les tâches dans des processus locaux séparés. <p>La valeur par défaut est OUT_OF_PROCESS.</p>
ExecutionOptions.RejectFilesDirectory	<p>Répertoire des fichiers de rejet. Les fichiers de rejet contiennent des lignes qui ont été rejetées lors de l'exécution d'un mappage. La valeur par défaut est <code><home directory>/reject</code>.</p> <p>Vous ne pouvez pas utiliser les caractères suivants dans le chemin du répertoire :</p> <p>* ? < > " ,</p>
ExecutionOptions.SourceDirectory	<p>Répertoire des fichiers plats source utilisés dans un mappage. La valeur par défaut est <code><home directory>/source</code>.</p> <p>Si le service d'intégration de données s'exécute sur une grille, utilisez un répertoire partagé pour créer un répertoire de fichiers source. Si vous configurez un répertoire différent pour chaque nœud doté du rôle de calcul, vérifiez que les fichiers source sont cohérents entre tous les répertoires source.</p> <p>Vous ne pouvez pas utiliser les caractères suivants dans le chemin du répertoire :</p> <p>* ? < > " ,</p>

Option	Description
ExecutionOptions.TargetDirectory	<p>Répertoire par défaut des fichiers plats cibles utilisés dans un mappage. La valeur par défaut est <code><home directory>/target</code>.</p> <p>Entrez une liste de répertoires séparés par des points-virgules afin d'augmenter les performances lorsque plusieurs partitions écrivent dans la cible du fichier plat.</p> <p>Si le service d'intégration de données s'exécute sur une grille, utilisez un répertoire partagé pour créer un répertoire de fichiers cibles. Si vous configurez un répertoire différent pour chaque nœud doté du rôle de calcul, vérifiez que les fichiers cibles sont cohérents entre tous les répertoires cibles.</p> <p>Vous ne pouvez pas utiliser les caractères suivants dans le chemin du répertoire :</p> <p>* ? < > " ,</p>
ExecutionOptions.TemporaryDirectories	<p>Répertoire de fichiers temporaires créés lors de l'exécution des tâches. La valeur par défaut est <code><home directory>/disTemp</code>.</p> <p>Entrez une liste de répertoires séparés par des points-virgules afin d'optimiser les performances pendant les opérations de profil et pendant le partitionnement du cache des transformations Trieur.</p> <p>Vous ne pouvez pas utiliser les caractères suivants dans le chemin du répertoire :</p> <p>* ? < > " , []</p>
HttpConfigurationOptions.AllowedHostNames	<p>Liste de constantes ou de modèles d'expressions régulières Java comparés au nom d'hôte de l'ordinateur associé à la demande. Les noms d'hôte sont sensibles à la casse. Utilisez une espace pour séparer plusieurs constantes ou expressions.</p> <p>Si vous configurez cette propriété, le service d'intégration de données accepte des demandes provenant de noms d'hôtes qui correspondent au modèle de nom d'hôte autorisé. Si vous ne configurez pas cette propriété, le service d'intégration de données utilise la propriété « Noms d'hôtes refusés » pour déterminer les clients qui peuvent envoyer des demandes.</p>
HttpConfigurationOptions.AllowedIPAddresses	<p>Liste de constantes ou de modèles d'expressions régulières Java comparés à l'adresse IP de l'ordinateur associé à la demande. Utilisez une espace pour séparer plusieurs constantes ou expressions.</p> <p>Si vous configurez cette propriété, le service d'intégration de données accepte les demandes provenant d'adresses IP qui correspondent au modèle d'adresse autorisé. Si vous ne configurez pas cette propriété, le service d'intégration de données utilise la propriété « Adresses IP refusées » pour déterminer les clients qui peuvent envoyer des demandes.</p>

Option	Description
HttpConfigurationOptions.DeniedHostNames	<p>Liste de constantes ou de modèles d'expressions régulières Java comparés au nom d'hôte de l'ordinateur associé à la demande. Les noms d'hôte sont sensibles à la casse. Utilisez une espace pour séparer plusieurs constantes ou expressions.</p> <p>Si vous configurez cette propriété, le service d'intégration de données accepte les demandes provenant de noms d'hôtes qui ne correspondent pas au modèle de nom d'hôte refusé. Si vous ne configurez pas cette propriété, le service d'intégration de données utilise la propriété « Noms d'hôtes autorisés » pour déterminer les clients qui peuvent envoyer des demandes.</p>
HttpConfigurationOptions.DeniedIPAddresses	<p>Liste de constantes ou de modèles d'expressions régulières Java comparés à l'adresse IP de l'ordinateur associé à la demande. Utilisez une espace pour séparer plusieurs constantes ou expressions.</p> <p>Si vous configurez cette propriété, le service d'intégration de données accepte les demandes provenant d'adresses IP qui ne correspondent pas au modèle d'adresse refusé. Si vous ne configurez pas cette propriété, le service d'intégration de données utilise la propriété « Adresses IP autorisées » pour déterminer les clients qui peuvent envoyer des demandes.</p>
HttpConfigurationOptions.HTTPProtocolType	<p>Protocole de sécurité utilisé par le service d'intégration de données. Entrez l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> - HTTP. Les demandes effectuées auprès du service doivent utiliser une URL HTTP. - HTTPS. Les demandes effectuées auprès du service doivent utiliser une URL HTTPS. - Les deux. Les demandes effectuées auprès du service peuvent utiliser une URL HTTP ou HTTPS. <p>Lorsque vous définissez le type de protocole HTTP sur HTTPS ou Les deux, vous devez activer TLS (Transport Layer Security) pour le service.</p> <p>Vous pouvez également activer le protocole TLS pour chaque service Web déployé vers une application. Lorsque vous activez le protocole HTTPS pour le service d'intégration de données et activez le protocole TLS pour le service Web, celui-ci utilise une URL HTTPS. Lorsque vous activez le protocole HTTPS pour le service d'intégration de données et n'activez pas le protocole TLS pour le service Web, celui-ci peut utiliser une URL HTTP ou HTTPS. Si vous activez TLS pour un service Web et n'activez pas le protocole HTTPS pour le service d'intégration de données, le service Web ne démarre pas.</p> <p>La valeur par défaut est HTTP.</p>
HttpProxyServerOptions.HttpProxyServerDomain	Domaine pour l'authentification.
HttpProxyServerOptions.HttpProxyServerHost	Nom du serveur proxy HTTP.
HttpProxyServerOptions.HttpProxyServerPassword	Mot de passe de l'utilisateur authentifié. Le gestionnaire de service crypte le mot de passe. Requis si le serveur proxy nécessite une authentification.
HttpProxyServerOptions.HttpProxyServerPort	<p>Numéro de port du serveur proxy HTTP.</p> <p>La valeur par défaut est 8080.</p>

Option	Description
HttpProxyServerOptions.HttpServerUser	Nom d'utilisateur authentifié pour le serveur proxy HTTP. Requis si le serveur proxy nécessite une authentification.
LoggingOptions.LogLevel	Niveau des messages d'erreur consigné par le service d'intégration de données dans le journal du service. Choisissez l'un des niveaux de message suivants : Irrécupérable, Erreur, Avertissement, Informations, Trace ou Déboguer.
MappingServiceOptions.MaxMemPerRequest	<p>Le comportement de la propriété Mémoire maximale par demande dépend des configurations suivantes du service d'intégration de données :</p> <ul style="list-style-type: none"> - Le service exécute les tâches dans des processus locaux ou distants distincts ou la propriété de service Taille maximale de la mémoire est définie sur 0 (valeur par défaut). Dans ce cas, la mémoire maximale par demande correspond à la quantité maximale de mémoire, en octets, que le service d'intégration de données peut allouer à toutes les transformations qui utilisent le mode de cache automatique dans une seule demande. Le service alloue de la mémoire séparément aux transformations qui disposent d'une taille du cache spécifique. La mémoire totale utilisée par la demande peut dépasser la valeur Mémoire maximale par demande. - Le service exécute les tâches dans le processus de service d'intégration de données et la valeur de la propriété de service Taille maximale de la mémoire est supérieure à 0. Dans ce cas, la mémoire maximale par demande correspond à la quantité maximale de mémoire, en octets, que le service d'intégration de données peut allouer à une seule demande. La mémoire totale utilisée par la demande ne peut pas dépasser la valeur Mémoire maximale par demande. <p>La valeur par défaut est 536 870 912.</p>
MappingServiceOptions.MaxNotificationThreadPoolSize	Alloue le nombre de threads qui envoient des notifications au client.
Modules.MappingService	Entrez False pour désactiver le module qui exécute les mappages et les aperçus. La valeur par défaut est True.
Modules.ProfilingService	Entrez False pour désactiver le module qui exécute des profils et génère des fiches d'évaluation. La valeur par défaut est True.
Modules.RESTService	Entrez False pour désactiver le module qui exécute le service Web REST. La valeur par défaut est True.
Modules.SQLService	Entrez False pour désactiver le module qui exécute des requêtes SQL sur un service de données SQL. La valeur par défaut est True.
Modules.WebService	Entrez False pour désactiver le module qui exécute les mappages d'opérations de service Web. La valeur par défaut est True.
Modules.WorkflowOrchestrationService	Entrez False pour désactiver le module qui exécute les flux de travail. La valeur par défaut est True.

Option	Description
PassThroughSecurityOptions.AllowCaching	Autorise la mise en cache de l'objet de données pour toutes les connexions d'intercommunication du service d'intégration de données. Remplit le cache de l'objet de données en utilisant les justificatifs d'identité présents dans l'objet de connexion. Remarque: Lorsque vous activez la mise en cache de l'objet de données avec la sécurité d'intercommunication, vous pouvez autoriser un accès non autorisé à certaines données.
ProfilingServiceOptions.ExportPath	Emplacement pour l'exportation des résultats de profil. Entrez le chemin du système de fichiers. La valeur par défaut est ./ProfileExport.
ProfilingServiceOptions.MaxExecutionConnections	Nombre maximal de connexions de base de données pour chaque tâche de profilage.
ProfilingServiceOptions.MaxPatterns	Nombre maximal de modèles à afficher pour un profil.
ProfilingServiceOptions.MaxProfileExecutionPoolSize	Nombre maximal de threads pour exécuter le profilage.
ProfilingServiceOptions.MaxRanks	Nombre de valeurs minimales et maximales à afficher pour un profil. La valeur par défaut est 5. La valeur par défaut est 10.
ProfilingServiceOptions.ProfileWarehouseConnectionName	Nom d'objet de connexion pour la connexion à l'entrepôt de profilage.
RepositoryOptions.RepositoryPassword	Mot de passe pour l'accès au référentiel modèle.
RepositoryOptions.RepositorySecurityDomain	Nom du domaine de sécurité LDAP si vous utilisez LDAP. Si vous n'utilisez pas LDAP, le domaine par défaut est natif.
RepositoryOptions.RepositoryServiceName	Service qui stocke les métadonnées d'exécution requises pour exécuter des mappages et des services de données SQL.
RepositoryOptions.RepositoryUserName	Nom d'utilisateur pour l'accès au référentiel modèle. L'utilisateur doit avoir le privilège Créer un projet pour le service de référentiel modèle.
ResultSetCacheOptions.EnableEncryption	Indique si les fichiers de cache de l'ensemble de résultats sont cryptés via le cryptage AES 128 bits. Les valeurs valides sont True ou False. La valeur par défaut est True.
ResultSetCacheOptions.FileNamePrefix	Préfixe des noms de tous les fichiers de cache de l'ensemble de résultats stockés sur le disque. La valeur par défaut est RSCACHE.

Option	Description
SQLServiceOptions.DTMKeepAliveTime	<p>Délai en millisecondes pendant lequel le processus DTM demeure ouvert après le traitement de la dernière demande. Les demandes SQL identiques peuvent réutiliser le processus ouvert.</p> <p>Utilisez l'intervalle de temps Garder actif pour améliorer les performances lorsque le délai requis pour traiter la requête SQL est limité par rapport au délai d'initialisation du processus DTM. Si la requête échoue, le processus DTM s'interrompt. Doit être supérieur ou égal à 0. 0 signifie que le service d'intégration de données ne conserve pas le processus DTM en mémoire. La valeur par défaut est 0.</p> <p>Vous pouvez également définir cette propriété pour chaque service de données SQL déployé dans le service d'intégration de données. Si vous définissez cette propriété pour un service de données SQL déployé, la valeur du service de données SQL déployé remplace la valeur que vous définissez pour le service d'intégration de données.</p>
SQLServiceOptions.MaxMemPerRequest	<p>Le comportement de la propriété Mémoire maximale par demande dépend des configurations suivantes du service d'intégration de données :</p> <ul style="list-style-type: none"> - Le service exécute les tâches dans des processus locaux ou distants distincts ou la propriété de service Taille maximale de la mémoire est définie sur 0 (valeur par défaut). Dans ce cas, la mémoire maximale par demande correspond à la quantité maximale de mémoire, en octets, que le service d'intégration de données peut allouer à toutes les transformations qui utilisent le mode de cache automatique dans une seule demande. Le service alloue de la mémoire séparément aux transformations qui disposent d'une taille de cache spécifique. La mémoire totale utilisée par la demande peut dépasser la valeur Mémoire maximale par demande. - Le service exécute les tâches dans le processus de service d'intégration de données et la valeur de la propriété de service Taille maximale de la mémoire est supérieure à 0. Dans ce cas, la mémoire maximale par demande correspond à la quantité maximale de mémoire, en octets, que le service d'intégration de données peut allouer à une seule demande. La mémoire totale utilisée par la demande ne peut pas dépasser la valeur Mémoire maximale par demande. <p>La valeur par défaut est 50 000 000.</p>
SQLServiceOptions.SkipLogFiles	<p>Empêche le service d'intégration de données de générer des fichiers journaux lorsque la demande du service de données SQL est traitée correctement et que le niveau de traçage est défini sur INFO ou sur un niveau supérieur. La valeur par défaut est False.</p>
SQLServiceOptions.TableStorageConnection	<p>Connexion de base de données relationnelle qui stocke les tables temporaires des services de données SQL. Par défaut, aucune connexion n'est sélectionnée.</p>
WorkflowOrchestrationServiceOptions.DBName	<p>Nom de connexion de la base de données qui stocke les métadonnées d'exécution des flux de travail.</p>

Option	Description
WorkflowOrchestrationServiceOptions.MaxWorkerThreads	<p>Nombre maximal de threads que le service d'intégration de données peut utiliser pour exécuter des tâches parallèles entre une paire de passerelles inclusives dans un flux de travail. La valeur par défaut est 10.</p> <p>Si le nombre de tâches entre les passerelles inclusives est supérieur à la valeur maximale, le service d'intégration de données exécute les tâches dans des lots que la valeur spécifie. Par exemple, si la valeur maximale des threads de travail est 10, le service d'intégration de données exécute les tâches en lots de dix.</p>
WSServiceOptions.DTMKeepAliveTime	<p>Délai en millisecondes pendant lequel le processus DTM demeure ouvert après le traitement de la dernière demande. Les demandes de service Web émises dans la même opération peuvent réutiliser le processus ouvert.</p> <p>Utilisez l'intervalle de temps Garder actif pour améliorer les performances lorsque le délai requis pour traiter la demande est limité par rapport au délai d'initialisation du processus DTM. Si la demande échoue, le processus DTM s'interrompt. Doit être supérieur ou égal à 0. 0 signifie que le service d'intégration de données ne conserve pas le processus DTM en mémoire. La valeur par défaut est 5 000.</p> <p>Vous pouvez également définir cette propriété pour chaque service Web déployé dans le service d'intégration de données. Si vous définissez cette propriété pour un service Web déployé, la valeur de ce service remplace la valeur que vous définissez pour le service d'intégration de données.</p>
WSServiceOptions.MaxMemPerRequest	<p>Le comportement de la propriété Mémoire maximale par demande dépend des configurations suivantes du service d'intégration de données :</p> <ul style="list-style-type: none"> - Le service exécute les tâches dans des processus locaux ou distants distincts ou la propriété de service Taille maximale de la mémoire est définie sur 0 (valeur par défaut). <p>Dans ce cas, la mémoire maximale par demande correspond à la quantité maximale de mémoire, en octets, que le service d'intégration de données peut allouer à toutes les transformations qui utilisent le mode de cache automatique dans une seule demande. Le service alloue de la mémoire séparément aux transformations qui disposent d'une taille de cache spécifique. La mémoire totale utilisée par la demande peut dépasser la valeur Mémoire maximale par demande.</p> - Le service exécute les tâches dans le processus de service d'intégration de données et la valeur de la propriété de service Taille maximale de la mémoire est supérieure à 0. <p>Dans ce cas, la mémoire maximale par demande correspond à la quantité maximale de mémoire, en octets, que le service d'intégration de données peut allouer à une seule demande. La mémoire totale utilisée par la demande ne peut pas dépasser la valeur Mémoire maximale par demande.</p> <p>La valeur par défaut est 50 000 000.</p>

Option	Description
WSServiceOptions.SkipLogFiles	Empêche le service d'intégration de données de générer des fichiers journaux lorsque la demande du service Web s'effectue correctement et que le niveau de traçage du service web est défini sur INFO ou sur un niveau supérieur. La valeur par défaut est False.
WSServiceOptions.WSDLLogicalURL	Préfixe de l'URL WSDL en cas d'utilisation d'un équilibrage de charge HTTP. Par exemple : http://loadbalancer:8080 Le service d'intégration de données requiert un équilibrage de charge HTTP pour exécuter un service Web sur une grille. Si vous exécutez le service d'intégration de données sur un nœud unique, il n'est pas nécessaire d'indiquer l'URL logique.

UpdateServiceProcessOptions

Met à jour les propriétés d'un processus de service d'intégration de données. Pour afficher les propriétés actuelles, exécutez la commande `infacmd` dis `ListServiceProcessOptions`.

Entrez les options en utilisant le format suivant :

```
... -o option_name=value option_name=value ...
```

Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

La commande `infacmd` dis `UpdateServiceProcessOptions` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments de la commande `infacmd dis UpdateServiceProcessOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
NodeName -nn	node_name	Requis. Nœud d'exécution du service d'intégration de données.
-Options -o	options	Requis. Entrez chaque option en la séparant par un espace. Pour afficher les options, exécutez la commande infacmd dis ListServiceProcessOptions.

Options du processus de service d'intégration de données

Utilisez les options du processus de service d'intégration de données avec la commande infacmd dis UpdateServiceProcessOptions.

Entrez les options du processus de service d'intégration de données au format suivant :

- Séparez les options multiples par un espace.
- Placez toutes les options et valeurs entre guillemets doubles.
- Placez les paramètres entre guillemets simples.

```
... -o "option_type.option_name='value'"
```

Le tableau suivant décrit les options du processus de service d'intégration de données :

Option	Description
GeneralOptions.JVMOptions	Options de ligne de commande de la machine virtuelle Java (JVM) pour l'exécution de programmes Java. Lorsque vous configurez les options JVM, vous devez définir le chemin de classe, ainsi que la mémoire minimale et maximale Java SDK.
GeneralOptions.HttpPort	Numéro de port HTTP unique pour le processus de service d'intégration de données lorsque le service utilise le protocole HTTP.
GeneralOptions.HttpsPort	Numéro de port HTTPS unique pour le processus de service d'intégration de données lorsque le service utilise le protocole HTTPS.
LoggingOptions.LogDirectory	Répertoire des journaux du processus de nœud du service d'intégration de données. La valeur par défaut est <INFA_HOME>\logs\dislogs. Si le service d'intégration de données s'exécute sur une grille, utilisez un répertoire partagé pour créer un répertoire de fichiers journaux unique. Utilisez un répertoire partagé pour vous assurer que le nouveau processus de service principal peut accéder aux fichiers journaux précédents en cas de basculement du processus vers un autre nœud.
ResultSetCacheOptions.MaxTotalDiskSize	Nombre maximal d'octets autorisés pour le stockage total du fichier de cache de l'ensemble de résultats. La valeur par défaut est 0.
ResultSetCacheOptions.MaxPerCacheMemorySize	Nombre maximal d'octets alloués pour une instance unique de cache de l'ensemble de résultats dans la mémoire. La valeur par défaut est 0.

Option	Description
ResultSetCacheOptions.MaxTotalMemorySize	Nombre maximal d'octets alloués pour le stockage total de cache de l'ensemble de résultats dans la mémoire. La valeur par défaut est 0.
ResultSetCacheOptions.MaxNumCaches	Nombre maximal d'instances de cache de l'ensemble de résultats autorisées pour ce processus de service d'intégration de données. La valeur par défaut est 0.
HttpConfigurationOptions.MaxConcurrentRequests	Nombre maximal de connexions HTTP ou HTTPS pouvant être établies à ce processus de service d'intégration de données. La valeur minimale est 4. La valeur par défaut est 200.
HttpConfigurationOptions.MaxBacklogRequests	Nombre maximal de connexions HTTP ou HTTPS pouvant patienter dans une file d'attente pour ce processus de service d'intégration de données. La valeur par défaut est 100.
HttpConfigurationOptions.KeyStoreFile	<p>Chemin et nom du fichier keystore contenant les clés et les certificats requis si vous utilisez le protocole HTTPS pour le service d'intégration de données. Vous pouvez créer un fichier keystore à l'aide d'un utilitaire keytool. keytool est un utilitaire qui génère et stocke des paires de clés privées ou publiques et les certificats associés dans un fichier keystore. Vous pouvez utiliser le certificat auto-signé ou un certificat signé par une autorité de certification.</p> <p>Si vous exécutez le service d'intégration de données sur une grille, le fichier keystore de chaque nœud de la grille doit contenir les mêmes clés.</p>
HttpConfigurationOptions.KeyStorePassword	Mot de passe du fichier keystore.
HttpConfigurationOptions.TrustStoreFile	<p>Chemin et nom du fichier Truststore contenant les certificats d'authentification approuvés par le service d'intégration de données.</p> <p>Si vous exécutez le service d'intégration de données sur une grille, le fichier Truststore de chaque nœud de la grille doit contenir les mêmes clés.</p>
HttpConfigurationOptions.TrustStorePassword	Mot de passe du fichier Truststore.
HttpConfigurationOptions.SSLProtocol	Protocole Secure Sockets Layer à utiliser. La valeur par défaut est TLS.
SQLServiceOptions.MaxConcurrentConnections	Limite le nombre de connexions à la base de données que le service d'intégration de données peut effectuer pour les services de données SQL. La valeur par défaut est 100.

Règles et directives

Reportez-vous aux règles et directives d'utilisation des commandes infacmd dis.

Tenez compte des règles et directives suivantes lorsque vous utilisez les commandes infacmd dis :

Règles et directives générales

- L'attribut de fuseau horaire accepte uniquement les valeurs de `java.time.ZoneID()`. Par exemple, `IST` n'est pas pris en charge.
- Les mots de passe chiffrés à l'aide de l'utilitaire `pmppasswd` doivent l'être à l'aide de l'option `-e=CRYPT_SYSTEM`.
- Vous devez disposer des autorisations de lecture sur un objet pour pouvoir l'interroger.
- Vous ne pouvez pas interroger des objets supprimés, même s'ils font partie d'une liste de changements en attente sur un référentiel modèle intégré à un système de contrôle de version.
- Lorsque vous comparez deux mappages, le rapport de comparaison imprime un blanc.
- Lorsque vous comparez deux mappages et utilisez Blaze comme environnement d'exécution, le rapport de comparaison indique le moteur comme `CADYarnExecutionEngine` au lieu de `Blaze`.

Règles et directives du correctif d'application

- Lorsque vous déployez des objets vers un fichier d'archive de correctif d'application, l'emplacement par défaut du fichier est `$INFA_HOME/tomcat/bin/target`. Si le service d'intégration de données est configuré pour utiliser des profils de système d'exploitation et que vous spécifiez le profil de système d'exploitation, le fichier d'archive est enregistré dans `$DISTargetDir` à la place.

CHAPITRE 14

Requêtes infacmd dis

Ce chapitre comprend les rubriques suivantes :

- [Requêtes, 280](#)
- [Opérateurs de comparaison, 281](#)
- [Opérateurs logiques, 283](#)
- [Paramètres de requête, 283](#)
- [Structure de requête, 285](#)
- [Clause Where, 286](#)

Requêtes

Utilisez les requêtes pour récupérer les objets de phase de conception et d'exécution.

Vous pouvez récupérer les objets de phase de conception à partir d'un référentiel modèle ou les objets d'exécution déployés sur un service d'intégration de données. Pour générer une requête, utilisez les paramètres de requête afin de déterminer les objets à récupérer. Vous pouvez créer une requête plus spécifique à l'aide de la clause Where et d'opérateurs.

Les commandes suivantes acceptent une requête en tant qu'option de ligne de commande :

- compareMapping
- deployObjectsToFile
- queryRunTimeObjects
- queryDesignTimeObjects
- replaceAllTag
- tag
- untag

Lorsque vous transmettez une requête à une commande, celle-ci opère uniquement sur les objets renvoyés par la requête. Si vous transmettez la requête `name=mapping1` à la commande `infacmd dis tag`, celle-ci attribue les balises uniquement aux objets portant le nom `mapping1`.

Pour transmettre une requête aux commandes, spécifiez la requête sous la forme d'une chaîne. Par exemple, reportez-vous à la valeur de l'option -q dans la syntaxe de la commande infacmd dis queryDesignTimeObjects suivante :

```
./infacmd.sh dis queryDesignTimeObjects -dn Domain_v299 -un Administrator
-pd Administrator -rs MRS_v299 -rsun Administrator -rspd Administrator
-q "all" -sn DIS_v299
```

Opérateurs de comparaison

Pour générer une requête, utilisez les opérateurs de comparaison avec les paramètres de requête. Vous pouvez utiliser des opérateurs de comparaison pour spécifier des critères lorsque vous interrogez des objets.

Le tableau suivant répertorie les opérateurs de comparaison que vous pouvez utiliser avec chaque type de paramètre de requête :

Type de paramètre de requête	Inclut les paramètres de requête	Opérateurs de comparaison	Exemples
Objet	name Balise createdBy lastModifiedBy	~contains~ ~not-contains~ ~not-ends-with~ ~not-starts-with~ ~ends-with~ ~starts-with~ = != ~in~ ~not-in~	name ~contains~ Mapping tag ~in~ (tg_1, tg_2, tg_3) createdBy = Administrator lastModifiedBy ~ends-with~ visitor
Objet	object type	= != ~in~ ~not-in~	type = Mapping object != Mapping object_in(P1/F1/Map1,P2/F1/Map2)
Heure	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 (days)

Type de paramètre de requête	Inclut les paramètres de requête	Opérateurs de comparaison	Exemples
Statut	versionStatus	~is-checkedin~ ~is-checkedout~	versionStatus ~is-checkedin~ versionStatus ~is-checkedout~
Emplacement	folder project application	~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)

Si vous avez généré une requête spécifiant un critère en utilisant des opérateurs de comparaison, la requête renvoie au client l'objet répondant au critère.

Par exemple, vous pouvez générer une requête pour récupérer des objets dont le nom est `mapping 1`.

```
name=mapping1
```

Remarque: Le format de date et d'heure est YYYY-MM-DD HH24:MI:SS.

Spécification d'un chemin de dossier

Utilisez un chemin de dossier récursif ou non récursif pour créer une requête. Vous pouvez spécifier le chemin du dossier pour accéder aux objets qui s'y trouvent.

Vous pouvez utiliser les types de chemin de dossier suivants :

- Récursif. Inclut des objets dans le dossier et tous les sous-dossiers.
- Non-récursif. N'inclut que les objets dans le dossier racine.

Les chemins de dossiers sont récursifs par défaut. Pour spécifier un chemin de dossier non récursif, utilisez une barre oblique à la fin du chemin de dossier.

Le tableau suivant décrit des exemples de requêtes avec des chemins de dossiers récursifs et non récursifs :

Exemple de requête	Description
name=map1 folder=/ 	Non-récursif. La requête examine uniquement les objets imbriqués directement sous le projet.
name=map1 folder=/f1/f2/	Non-récursif. La requête examine uniquement les objets dans le chemin /f1/f2/.

Exemple de requête	Description
name=map1 folder=f1	Récuratif. La requête examine uniquement les objets dans le dossier f1 et tous les sous-dossiers qui s'y trouvent.
name=map1 folder=/f1/f2	Récuratif. La requête examine tous les objets dans le chemin /f1/f2 et tous les sous-dossiers qui se trouvent dans f2.

Remarque: Si vous utilisez une barre oblique pour spécifier un chemin de dossier non récursif, vous pouvez uniquement utiliser les opérateurs de comparaison =, !=, ~in~ et ~not-in~.

Opérateurs logiques

Utilisez des opérateurs logiques pour tester si une ou plusieurs conditions d'une requête sont TRUE ou FALSE.

Vous pouvez utiliser les opérateurs logiques suivants :

Opérateur logique	Description	Exemple
!	NOT	! name ~not-starts-with~ M_
&&	AND	name ~starts-with~ map_&& lastModifiedBy ~ends-with~ visitor
	OU	checkInTime > 2018-12-26 20:32:54 lastModifiedTime > 2019-02-26 20:32:54

Remarque: Vous ne pouvez pas utiliser d'opérateurs logiques pour tester les paramètres de requête d'emplacement, y compris les noms de dossier, les noms de projet et les noms d'application.

Paramètres de requête

Utilisez les paramètres de requête pour interroger les objets en phase de conception dans un référentiel modèle et les objets d'exécution déployés dans un service d'intégration de données. Vous pouvez générer une requête à l'aide des éléments suivants : objet, heure, statut et emplacement.

Ils sont répartis selon les types suivants :

Objet

Paramètres qui testent un objet tel qu'un objet ou un utilisateur spécifique. Le tableau suivant répertorie les paramètres d'objet :

Paramètre	Type d'objet	Description
name	Objet de phase de conception Objet d'exécution	Nom de l'objet à interroger. Vous pouvez spécifier le nom de l'un des types d'objet suivants : <ul style="list-style-type: none">- Mappage- Objet de données physique- Ensemble de paramètres
tag	Objet de phase de conception	Balise attribuée à l'objet.
createdBy	Objet de phase de conception	Utilisateur ayant créé l'objet.
lastModifiedBy	Objet de phase de conception	Auteur de la dernière modification de l'objet.
type	Objet de phase de conception	Filtre le type d'objet.
object	Objet de phase de conception	Filtre et récupère les objets d'un dossier. Spécifiez le chemin d'accès complet aux objets à partir de la racine, y compris le nom du projet, les dossiers et le nom de l'objet.

Heure

Paramètres qui testent l'heure de modification d'un objet. Le tableau suivant répertorie les paramètres d'heure :

Paramètre	Type d'objet	Description
lastModifiedTime	Objet de phase de conception	Heure à laquelle l'objet a été modifié pour la dernière fois.
checkInTime	Objet de phase de conception	Heure à laquelle l'objet a été archivé pour la dernière fois. Remarque: Ne s'applique que si le référentiel modèle est intégré à un système de contrôle de versions.
checkOutTime	Objet de phase de conception	Heure à laquelle l'objet a été extrait pour la dernière fois. Remarque: Ne s'applique que si le référentiel modèle est intégré à un système de contrôle de versions.
creationTime	Objet de phase de conception	Heure à laquelle l'objet a été créé.

Statut

Paramètres qui testent le statut d'un objet. Le tableau suivant répertorie les paramètres de statut :

Paramètre	Type d'objet	Description
versionStatus	Objet de phase de conception	Statut de la version de l'objet. Le statut de la version peut être Archivé ou Extrait. Remarque: Ne s'applique que si le référentiel modèle est intégré à un système de contrôle de versions.

Emplacement

Paramètres qui testent l'emplacement d'un objet, tel qu'un projet, un dossier ou une application d'exécution spécifique. Le tableau suivant répertorie les paramètres d'emplacement :

Paramètre	Type d'objet	Description
folder	Objet de phase de conception	Dossier qui contient l'objet.
project	Objet de phase de conception	Projet qui contient l'objet.
application	Objet d'exécution	Nom de l'application d'exécution qui contient l'objet.

Structure de requête

Utilisez des paramètres, des opérations et la clause Where pour générer une requête.

Vous pouvez structurer une requête à l'aide de paramètres, d'opérateurs de comparaison, d'opérateurs logiques et de la clause Where. Vous pouvez contrôler la priorité des requêtes en utilisant des parenthèses.

Une requête est structurée à l'aide des éléments suivants :

Paramètres de la requête

Les paramètres de la requête sont catégorisés en objet, heure, statut et emplacement. Chaque paramètre de requête doit être combiné avec un opérateur de comparaison. Par exemple :

```
mapping=Mapping1
```

Opérateurs de comparaison

Les opérateurs de comparaison sont utilisés pour spécifier des critères pour interroger les objets. Ils sont utilisés avec les paramètres permettant de créer une requête.

Opérateurs logiques

Les opérateurs logiques sont utilisés pour tester une condition d'une requête. Ils peuvent comporter plusieurs paramètres de requête. Par exemple :

```
mapping=Mapping1 || createdBy=admin
```

Clause Where

La clause Where est utilisée pour limiter la portée de la requête. Par exemple :

```
name=mapping1 where project=project1, folder=folder1.
```

Clause Where

Utilisez une clause Where pour limiter la portée d'une requête.

Vous pouvez spécifier des paramètres de requête d'emplacement uniquement dans une clause Where. Les paramètres de requête d'emplacement ne prennent pas en charge les opérateurs logiques. Vous ne pouvez donc pas utiliser ces derniers dans la clause Where.

Par exemple, la requête suivante localise un mappage dans un projet et un dossier spécifiques :

```
name=mapping1 where project1, folder=folder1
```

Vous pouvez utiliser des parenthèses en dehors de la clause Where. Par exemple, la requête suivante utilise les expressions `(name contains super && name ends-with boy)` et `(name contains ragnarok)` qui sont mises entre parenthèses en dehors de la clause Where :

```
(name contains super && name ends-with boy) || (name contains ragnarok) where  
project=MapGenTest
```

Vous pouvez utiliser le mot clé `all` pour localiser tous les objets en phase de conception sur un référentiel modèle ou tous les objets d'exécution déployés dans un service d'intégration de données. Vous pouvez utiliser le mot clé `all` avec la clause Where.

Par exemple, la requête suivante localise tous les objets dans un dossier spécifique :

```
all where folder=Folder_1
```

CHAPITRE 15

Référence de commande infacmd dp

Ce chapitre comprend les rubriques suivantes :

- [startSparkJobServer, 287](#)
- [stopSparkJobServer, 289](#)

startSparkJobServer

Démarre Spark Jobserver sur la machine du service d'intégration de données. Par défaut, Spark Jobserver démarre lorsque vous affichez l'aperçu des données hiérarchiques.

Exécutez cette commande pour démarrer manuellement Spark Jobserver en arrière-plan afin d'écourter les délais lorsque vous prévisualisez les données hiérarchiques.

La commande infacmd dp startSparkJobServer utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd dp startSparkJobServer` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation. Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec ces deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données.
-ConfigurationName -cn	configuration_name	Requis. Nom de la configuration du cluster.

stopSparkJobServer

Arrête l'instance de Spark Jobserver en cours d'exécution sur le service d'intégration de données spécifié. Par défaut, Spark Jobserver s'arrête s'il est inactif pendant 60 minutes ou si le service d'intégration de données est arrêté ou recyclé.

La commande infacmd dp startSparkJobServer utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande infacmd dp stopSparkJobServer :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p> <p>Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec ces deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données.

CHAPITRE 16

Référence de commande infacmd idp

Ce chapitre comprend les rubriques suivantes :

- [createRepository, 291](#)
- [createService, 293](#)
- [updateService, 297](#)
- [upgradeRepository, 300](#)

createRepository

Crée un référentiel de préparation de données.

La syntaxe de la commande infacmd idp createRepository est la suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd idp createRepository :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de préparation de données interactive associé au référentiel de préparation de données.

createService

Crée un service de préparation de données interactive.

La syntaxe de la commande infacmd idp createService est la suivante :

```
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(nonsecure|kerberos (default nonsecure)),IDLKerberosPrincipal(Principal Name for User Impersonation),IDLKerberosKeyTabFileName(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]

```

Le tableau suivant décrit les options et arguments d'infacmd idp createService :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>
-ServiceName -sn	service_name	<p>Requis. Nom du service de préparation de données interactive.</p> <p>Vous ne pouvez pas modifier le nom du service après sa création. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Il ne peut pas dépasser 128 caractères ni commencer par @. Il ne peut contenir ni espaces ni l'un des caractères spéciaux suivants :</p> <p>` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []</p>
-NodeName -nn	node_name	<p>Obligatoire si vous ne spécifiez pas le nom de la grille. Nœud sur lequel le service s'exécute.</p>
-BackupNodes -bn	node_name1,node_name2,...	<p>Facultatif. Nœuds sur lesquels le service peut s'exécuter si le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.</p>
-ServiceOptions -so	option_name=value ...	<p>Facultatif. Propriétés du service qui définissent le mode d'exécution du service.</p>

Option	Argument	Description
-LicenseName -ln	license_name	Facultatif. Objet de licence qui permet l'utilisation du service.
-RepositoryServiceName -rs	repository_service_name	Facultatif. Nom du service de référentiel modèle qui gère le référentiel modèle qui contient les objets et les métadonnées de règles. Définissez cette propriété si les règles sont utilisées lors de la préparation de données.
-RepositoryUser -rsun	-repository_username	Facultatif. Compte d'utilisateur à utiliser pour se connecter au service de référentiel modèle.
-RepositoryPassword -rspd	-repository_password	Facultatif. Mot de passe correspondant au compte d'utilisateur du service de référentiel modèle.
-RepositorySecurityDomain -rssdn	model_repository_security_domain	Facultatif. Domaine de sécurité auquel le service de référentiel modèle appartient.
-DISServiceName -dsn	dis_service_name	Facultatif. Nom du service d'intégration de données qui exécute les règles pendant la préparation de données. Définissez cette propriété si les règles sont utilisées lors de la préparation de données.
-HttpPort -hp	http_port	Obligatoire si vous ne spécifiez pas de port HTTPS. Numéro de port HTTP unique utilisé pour chaque processus de service d'intégration de données. Après avoir créé le service, vous pouvez définir des numéros de port différents pour chaque processus de service.
-HttpsPort -hsp	https_port	Obligatoire si vous ne spécifiez pas de port HTTP. Numéro de port HTTPS unique utilisé pour chaque processus de service d'intégration de données. Après avoir créé le service, vous pouvez définir des numéros de port différents pour chaque processus de service.
-KeystoreFile -kf	keystore_file_location	Facultatif. Chemin et nom du fichier keystore contenant les clés et les certificats requis si vous utilisez le protocole HTTPS pour le service. Vous pouvez créer un fichier keystore à l'aide de keytool. keytool est un utilitaire qui génère et stocke des paires de clés privées ou publiques et les certificats associés dans un fichier keystore. Vous pouvez utiliser le certificat auto-signé ou un certificat signé par une autorité de certification.

Option	Argument	Description
-KeystorePassword -kp	keystore_password	Facultatif. Mot de passe pour le fichier keystore
-TruststoreFile -tsf	truststore_file_location	Facultatif. Chemin d'accès et nom du fichier truststore contenant les certificats d'authentification requis pour la connexion HTTPS.
-TruststorePassword -tsp	truststore_password	Facultatif. Mot de passe pour le fichier truststore.
-RulesServerPort -rpo	RulesServerPort	Facultatif. Port utilisé par le serveur de règles géré par le service de préparation de données interactive. Définissez la valeur sur un port disponible sur le nœud où le service de s'exécute.
-SolrPort -spo	SolrPort	Facultatif. Numéro de port du serveur Apache Solr utilisé pour fournir des recommandations sur la préparation des données.
-maxHeapSize -mxhs	maxHeapSize	Facultatif. Taille des segments de mémoire à allouer au service.
-FolderPath -fp	full_folder_path	Facultatif. Chemin d'accès complet, sans le nom de domaine, du dossier dans lequel vous souhaitez créer le service. Doit être au format suivant : <i>/parent_folder/child_folder</i>

updateService

Met à jour les propriétés du service de préparation de données interactive.

La syntaxe de la commande infacmd idp updateService est la suivante :

```
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(nonsecure|kerberos
(default nonsecure)),IDLKerberosPrincipal(Principal Name for User
Impersonation),IDLKerberosKeyTabFileName(SPN Keytab File for User Impersonation),
LogAuditEvents(true|false (default
false)),JDBCPort,ZeppelinURL,MaxFileUploadSize(default=512MB),DownloadRowsSize(default=10
0000),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 ...)]

```

Le tableau suivant décrit les options et arguments d'infacmd idp updateService :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>
-ServiceName -sn	service_name	<p>Requis. Nom du service de préparation de données interactive.</p> <p>Vous ne pouvez pas modifier le nom du service après sa création. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Il ne peut pas dépasser 128 caractères ni commencer par @. Il ne peut contenir ni espaces ni l'un des caractères spéciaux suivants :</p> <p>` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []</p>
-ServiceOptions -so	option_name=value ...	<p>Facultatif. Propriétés du service qui définissent le mode d'exécution du service.</p>
-RepositoryServiceName -rs	repository_service_name	<p>Facultatif. Nom du service de référentiel modèle qui gère le référentiel modèle qui contient les objets et les métadonnées de règles. Définissez cette propriété si les règles sont utilisées lors de la préparation de données.</p>
-RepositoryUser -rsun	-repository_username	<p>Facultatif. Compte d'utilisateur à utiliser pour se connecter au service de référentiel modèle.</p>

Option	Argument	Description
-RepositoryPassword -rspd	-repository_password	Facultatif. Mot de passe correspondant au compte d'utilisateur du service de référentiel modèle.
-RepositorySecurityDomain -rssdn	model_repository_security_domain	Facultatif. Domaine de sécurité auquel le service de référentiel modèle appartient.
-DISServiceName -dsn	dis_service_name	Facultatif. Nom du service d'intégration de données qui exécute les règles pendant la préparation de données. Définissez cette propriété si les règles sont utilisées lors de la préparation de données.
-NodeName -nn	node_name	Obligatoire si vous ne spécifiez pas le nom de la grille. Nœud sur lequel le service s'exécute.
-BackupNodes -bn	node_name1,node_name2,...	Facultatif. Nœuds sur lesquels le service peut s'exécuter si le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.
-ServiceProcessOptions -po	option_name=value ...	Facultatif. Propriétés du processus de service pour le service Dans un environnement à nœuds multiples, infacmd applique ces propriétés au nœud principal et au nœud de sauvegarde.

upgradeRepository

Met à niveau le contenu d'un référentiel de préparation de données.

La commande infacmd idp upgradeRepository utilise la syntaxe suivante :

```

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

```


Le tableau suivant décrit les options et les arguments de la commande `infacmd idp upgradeRepository` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de préparation de données interactive associé au référentiel de préparation de données.

CHAPITRE 17

Référence de commande infacmd edp

Ce chapitre comprend les rubriques suivantes :

- [createService, 303](#)
- [purgeauditevents, 307](#)
- [updateService, 310](#)
- [upgradeService, 313](#)

createService

Crée un service Enterprise Data Preparation.

La syntaxe de la commande infacmd edp createService est la suivante :

```
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(nonsecure|kerberos (default nonsecure)),IDLKerberosPrincipal(Principal Name for User Impersonation),IDLKerberosKeyTabFileName(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]

```

Le tableau suivant décrit les options et arguments d'infacmd edp createService :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service Enterprise Data Preparation. Vous ne pouvez pas modifier le nom du service après sa création. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Il ne peut pas dépasser 128 caractères ni commencer par @. Il ne peut contenir ni espaces ni l'un des caractères spéciaux suivants : ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
-Description -des	description	Facultatif. Description du service.
-NodeName -nn	node_name	Obligatoire si vous ne spécifiez pas le nom de la grille. Nœud sur lequel le service s'exécute.

Option	Argument	Description
-BackupNodes -bn	node_name1,node_name2,...	Facultatif. Nœuds sur lesquels le service peut s'exécuter si le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.
-ServiceOptions -so	option_name=value ...	Facultatif. Propriétés de service qui définissent le mode d'exécution du service Enterprise Data Preparation.
-LicenseName -ln	license_name	Facultatif. Objet de licence qui permet l'utilisation du service.
-HttpPort -hp	http_port	Obligatoire si vous ne spécifiez pas de port HTTPS. Numéro de port HTTP unique utilisé pour chaque processus de service d'intégration de données. Après avoir créé le service, vous pouvez définir des numéros de port différents pour chaque processus de service.
-HttpsPort -hsp	https_port	Obligatoire si vous ne spécifiez pas de port HTTP. Numéro de port HTTPS unique utilisé pour chaque processus de service. Après avoir créé le service, vous pouvez définir des numéros de port différents pour chaque processus de service.
-KeystoreFile -kf	keystore_file_location	Facultatif. Chemin et nom du fichier keystore contenant les clés et les certificats requis si vous utilisez le protocole HTTPS pour le service. Vous pouvez créer un fichier keystore à l'aide de keytool. keytool est un utilitaire qui génère et stocke des paires de clés privées ou publiques et les certificats associés dans un fichier keystore. Vous pouvez utiliser le certificat auto-signé ou un certificat signé par une autorité de certification.
-KeystorePassword -kp	keystore_password	Facultatif. Mot de passe pour le fichier keystore
-TruststoreFile -tf	truststore_file_location	Facultatif. Chemin d'accès et nom du fichier truststore contenant les certificats d'authentification requis pour la connexion HTTPS.
-TruststorePassword -tp	truststore_password	Facultatif. Mot de passe pour le fichier truststore.
-FolderPath -fp	full_folder_path	Facultatif. Chemin d'accès complet, sans le nom de domaine, du dossier dans lequel vous souhaitez créer le service. Doit être au format suivant : <i>/parent_folder/child_folder</i>

Option	Argument	Description
-RepositoryService -rs	repository_service_name	Obligatoire. Nom du service de référentiel modèle à associer au service Enterprise Data Preparation.
-RepositoryUser -rsun	-repository_username	Obligatoire. Compte d'utilisateur à utiliser pour se connecter au service de référentiel modèle.
-RepositoryPassword -rspd	-repository_password	Facultatif. Mot de passe correspondant au compte d'utilisateur du service de référentiel modèle.
- RepositorySecurityDomain -rssdn	model_repository_security_domain	Facultatif. Domaine de sécurité auquel le service de référentiel modèle appartient.
- DataPreparationServiceName -dpsn	data_preparation_service_name	Obligatoire. Nom du service de préparation de données interactive à associer au service Enterprise Data Preparation.
-DISServiceName -dsn	dis_service_name	Obligatoire. Nom du service d'intégration de données à associer au service Enterprise Data Preparation.
-CatalogService -ct	catalog_service_name	Obligatoire. Nom du service de catalogue à associer au service Enterprise Data Preparation.
-CatalogServiceUser -ctun	catalogservice_user	Obligatoire. Compte d'utilisateur à utiliser pour se connecter au service de catalogue.
- CatalogServicePassword -ctpd	catalogservice_password	Facultatif. Mot de passe du compte d'utilisateur du service de catalogue.
- CatalogSecurityDomain -cssdn	catalog_security_domain	Facultatif. Domaine de sécurité auquel le service de catalogue appartient.

purgeauditevents

Purge tous les événements de l'activité utilisateur Enterprise Data Preparation de la base de données d'audit.
Purge en option les événements de l'historique du projet de la base de données d'audit.

Pour plus d'informations sur les événements consignés dans la base de données d'audit, consultez le *Guide de l'administrateur d'Informatica Enterprise Data Preparation*.

La syntaxe de la commande `infacmd edp purgeauditevents` est la suivante :

```

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]

```

Le tableau suivant décrit les options et arguments d'`infacmd edp purgeauditevents` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>
-ServiceName -sn	service_name	<p>Requis. Nom du service Enterprise Data Preparation pour lequel purger les événements.</p>
-AuditDataRetentionPeriod -Rp	audit_data_retention_period_in_weeks	<p>Requis. Nombre de semaines avant la semaine civile actuelle pendant laquelle les données d'événements sont conservées. La commande ne purge pas les données de la semaine civile actuelle.</p> <p>Spécifiez 0 pour conserver les données d'une semaine civile et purger les données du journal précédent.</p> <p>Spécifiez 1 au minimum pour conserver les données de n + 1 semaines civiles et purger les données du journal précédent.</p> <p>Si vous spécifiez 1, par exemple, la commande conserve les données de deux semaines civiles lorsqu'elle effectue la purge.</p> <p>La valeur minimale est 0.</p>
PurgeProjectHistoryEvent -phe	true false	<p>Facultatif. Purge les événements de l'historique du projet de la base de données d'audit.</p> <p>Définissez sur True afin de purger l'historique du projet de la base de données d'audit.</p> <p>La valeur par défaut est False.</p>

updateService

Met à jour un service Enterprise Data Preparation.

La syntaxe de la commande `infacmd edp updateService` est la suivante :

```
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(nonsecure|kerberos
(default nonsecure)),IDLKerberosPrincipal(Principal Name for User
Impersonation),IDLKerberosKeyTabFileName(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)

<-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]
```

Le tableau suivant décrit les options et arguments d'infacmd edp updateService :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service Enterprise Data Preparation. Vous ne pouvez pas modifier le nom du service après sa création. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Il ne peut pas dépasser 128 caractères ni commencer par @. Il ne peut contenir ni espaces ni l'un des caractères spéciaux suivants : ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
-ServiceOptions -so	option_name=value ...	Facultatif. Propriétés du service qui définissent le mode d'exécution du service.
-NodeName -nn	node_name	Obligatoire si vous ne spécifiez pas le nom de la grille. Nœud sur lequel le service s'exécute.
-BackupNodes -bn	node_name1,node_name2,...	Facultatif. Nœuds sur lesquels le service peut s'exécuter si le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.
-ServiceProcessOptions -po	option_name=value ...	Facultatif. Propriétés du processus de service pour le service Dans un environnement à nœuds multiples, infacmd applique ces propriétés au nœud principal et au nœud de sauvegarde.
-RepositoryService -rs	repository_service_name	Facultatif. Nom du service de référentiel modèle à associer au service Enterprise Data Preparation.
-RepositoryUser -rsun	-repository_username	Facultatif. Compte d'utilisateur à utiliser pour se connecter au service de référentiel modèle.
-RepositoryPassword -rspd	-repository_password	Facultatif. Mot de passe correspondant au compte d'utilisateur du service de référentiel modèle.
-RepositorySecurityDomain -rssdn	model_repository_security_domain	Facultatif. Domaine de sécurité auquel le service de référentiel modèle appartient.

Option	Argument	Description
- DataPreparationServiceName -dpsn	data_preparation_service_name	Facultatif. Nom du service de préparation de données interactive à associer au service Enterprise Data Preparation.
-DISServiceName -dsn	dis_service_name	Facultatif. Nom du service d'intégration de données à associer au service Enterprise Data Preparation.
-CatalogService -ct	nom_service_catalogue	Facultatif. Nom du service de catalogue à associer au service Enterprise Data Preparation.
-CatalogServiceUser -ctun	catalogservice_user	Facultatif. Compte d'utilisateur à utiliser pour se connecter au service de catalogue.
- CatalogServicePassword -ctpd	catalogservice_password	Facultatif. Mot de passe du compte d'utilisateur du service de catalogue.
- CatalogSecurityDomain -cssdn	catalog_security_domain	Facultatif. Domaine de sécurité auquel le service de catalogue appartient.

upgradeService

Met à niveau un service Enterprise Data Preparation.

La syntaxe de la commande infacmd edp upgradeService est la suivante :

```

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

```

Le tableau suivant décrit les options et arguments d'infacmd edp upgradeService :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service Enterprise Data Preparation à mettre à niveau.

CHAPITRE 18

Référence de commande infacmd es

Ce chapitre comprend les rubriques suivantes :

- [ListServiceOptions, 316](#)
- [UpdateServiceOptions, 317](#)
- [UpdateSMTPOptions, 318](#)

ListServiceOptions

Renvoie une liste de propriétés qui sont configurées pour le service de messagerie électronique. Pour configurer les propriétés du service de messagerie électronique, exécutez la commande `infacmd es updateServiceOptions`. Pour configurer les propriétés du serveur de messagerie du service de messagerie électronique, exécutez la commande `infacmd es updateSMTPOptions`.

La commande `infacmd es listServiceOptions` utilise la syntaxe suivante :

```
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]
```

Remarque: Le programme `infacmd` utilise les options courantes suivantes pour se connecter au domaine : nom de domaine, nom d'utilisateur, mot de passe, domaine de sécurité et délai de résilience. Le tableau d'options présente de brèves descriptions. Pour afficher des descriptions détaillées, reportez-vous à ["Connexion au domaine" à la page 66](#).

Le tableau suivant décrit les options et arguments de la commande `infacmd es listServiceOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-ServiceName -sn	service_name	Facultatif. Entrez Email_Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine.

UpdateServiceOptions

Met à jour les propriétés du service de messagerie électronique. Exécutez cette commande pour configurer les propriétés du domaine et les nœuds du service de messagerie électronique. Pour afficher les propriétés actuelles du service de messagerie électronique, exécutez la commande `infacmd es listServiceOptions`.

La commande `infacmd es updateServiceOptions` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande `infacmd es updateServiceOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-ServiceName -sn	service_name	Facultatif. Entrez Email_Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine.
-Options -o	options	Entrez les options en utilisant le format suivant : OptionGroupName.OptionName=OptionValue OptionGroupName2.OptionName2=OptionValue2 Pour afficher les options valides, exécutez la commande <code>infacmd isp ListServiceOptions</code> .
-NodeName -nn	primary node name	Facultatif. Nœud principal sur lequel le service s'exécute.
-BackupNodes -bn	noms du nœud de sauvegarde	Facultatif. Nœuds sur lesquels le service peut s'exécuter si le nœud principal n'est pas disponible.

UpdateSMTPOptions

Met à jour les propriétés SMTP du service de messagerie électronique. Les glossaires d'entreprise et les flux de travail utilisent la configuration SMTP du service de messagerie électronique pour les notifications par courriel.

Les notifications suivantes utilisent la configuration SMTP du service de messagerie électronique pour envoyer des courriels :

- Notifications de Business Glossary.
- Notifications de la fiche d'évaluation.
- Notifications de flux de travail. Les notifications de flux de travail incluent des courriels envoyés à partir de tâches humaines et des tâches de notification dans les flux de travail que le service d'intégration de données exécute.

La commande infacmd es updateSMTPOptions utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd es updateSMTPOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-ServiceName -sn	service_name	Facultatif. Entrez Email_Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine.
-SMTPServerHostName -sa	smtp_host	Facultatif. Nom d'hôte du serveur de messagerie sortant SMTP. Par exemple, entrez le serveur Microsoft Exchange Server pour Microsoft Outlook. La valeur par défaut est localhost.
-SMTPUsername -su	smtp_user	Facultatif. Nom d'utilisateur permettant l'authentification lors de l'envoi, si le serveur d'e-mail sortant l'exige.

Option	Argument	Description
-SMTPEmailPassword -se	smtp_email_password	Facultatif. Mot de passe pour l'authentification lors de l'envoi si le serveur d'e-mail SMTP sortant le requiert.
-SMTPEmailAddress -ss	smtp_email_address	Facultatif. Adresse de courriel utilisée par le service de messagerie électronique dans le champ De lors de l'envoi de courriels de notification à partir d'un flux de travail. La valeur par défaut est <code>admin@example.com</code> .
SMTPPort -sp	smtp_port	Facultatif. Numéro de port utilisé par le serveur de messagerie SMTP sortant. Les valeurs valides sont comprises entre 1 et 65 535. La valeur par défaut est 25.
-SMTPAuthEnabled -sau	smtp_auth_enabled	Facultatif. Indique que le serveur SMTP est activé pour l'authentification. S'il est défini sur <code>True</code> , le serveur de messagerie sortant requiert un nom d'utilisateur et un mot de passe. Si la valeur est <code>True</code> , vous devez sélectionner si le serveur utilise le protocole TLS (Transport Layer Security) ou le protocole SSL (Secure Sockets Layer). Entrez <code>True</code> ou <code>False</code> . La valeur par défaut est <code>False</code> .
-SMTPTLSEnabled -stls	smtp_tls_enabled	Facultatif. Indique que le serveur SMTP utilise le protocole TLS. S'il est défini sur <code>True</code> , entrez le numéro de port TLS comme propriété du port du serveur SMTP. Entrez <code>True</code> ou <code>False</code> . La valeur par défaut est <code>False</code> .
-SMTPSSLEnabled -sssl	smtp_ssl_enabled	Facultatif. Indique que le serveur SMTP utilise le protocole SSL. S'il est défini sur <code>True</code> , entrez le numéro de port SSL comme propriété du port du serveur SMTP. Entrez <code>True</code> ou <code>False</code> . La valeur par défaut est <code>False</code> .

CHAPITRE 19

Référence de commande infacmd ics

Ce chapitre comprend les rubriques suivantes :

- [cleanCluster, 321](#)
- [createservice, 323](#)
- [ListServiceOptions, 334](#)
- [ListServiceProcessOptions, 335](#)
- [shutdownCluster, 337](#)
- [UpdateServiceOptions, 338](#)
- [UpdateServiceProcessOptions, 340](#)

cleanCluster

Nettoie le service de cluster Informatica.

La syntaxe de la commande infacmd ics cleanCluster est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd ics cleanCluster` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de cluster Informatica.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

createservice

Crée un service de cluster Informatica.

La syntaxe de la commande `infacmd ics createService` est la suivante :

```
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|-sslp> 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> Zookeepr 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)]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd ics CreateService` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-NodeName -nn	node_name	Requis. Nom de nœud de domaine Informatica.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-UserName -un	user_name	<p>Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>

Option	Argument	Description
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de cluster Informatica.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-HttpPort -p	port_name	Facultatif. Numéro de port HTTP unique utilisé pour le service de cluster Informatica. Le numéro de port par défaut est 9075.
-HttpsPort -sp	https_port_name	Requis si vous activez le protocole TLS (Transport Layer Security). Numéro de port de la connexion HTTPS.
-KeystoreFile -kf	keystore_file_location	Requis si vous avez choisi d'activer le protocole TLS (Transport Layer Security). Chemin d'accès et nom du fichier keystore. Le fichier keystore contient les clés et les certificats requis si vous utilisez le protocole de sécurité SSL avec l'outil Catalog® Administrator.
-KeystorePassword -kp	keystore_password	Requis si vous avez choisi d'activer le protocole TLS (Transport Layer Security). Mot de passe du fichier keystore.
-SSLProtocol -sslp	ssl_protocol	Facultatif. Protocole SSL (Secure Sockets Layer) à utiliser.

Option	Argument	Description
-GatewayHost -hgh	gateway_host	Requis. Nom d'hôte du nom de domaine complet (FQDN) du nœud qui sert de passerelle au cluster Informatica.
-DataNodes -hn	data_nodes	Liste de noms d'hôte FQDN, séparés par des virgules, qui sont des nœuds de données du cluster Informatica. Obligatoire si la configuration avancée n'est pas activée.
-ProcessingNodes -pn	processing_nodes	Liste de noms d'hôte FQDN, séparés par des virgules, qui traitent les nœuds du cluster Informatica.
-GatewayUser -gu	gateway_user	Nom d'utilisateur pour le nœud de passerelle. Activez une connexion SSH sans mot de passe à partir du domaine Informatica vers l'hôte de passerelle pour l'utilisateur actuel. L'utilisateur doit être un utilisateur sudo non-racine.
-ClusterCustomDir -ccd	cluster_custom_dir	Répertoire du cluster personnalisé. Par exemple, la valeur par défaut est /opt/informatica/ics
-ClusterSharedFilesystemPath -csfp	cluster_shared_filesystem_path	Requis si le service de cluster Informatica est configuré sur plusieurs nœuds. Chemin du système de fichiers partagés du cluster.
-OtherOptions -oo	other_options	Plusieurs options pouvant être séparées par une virgule. Si la valeur d'une option contient une virgule, elle doit être spécifiée entre guillemets doubles. Le format requis est le suivant : [OptionGroupName.OptionName=OptionValue].
-BackupNodes -bn	node_name1,node_name2,...	Facultatif. Nœuds sur lesquels le service peut s'exécuter si le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.
-NomadServerHosts -nsh	nomad_server_hosts	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez les hôtes du serveur Nomad en les séparant par des virgules.

Option	Argument	Description
-NomadSerfPort -nsp	nomad_service_port	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez le port du serveur Nomad. La valeur par défaut est 4648.
-NomadHttpPort -nhp	nomad_http_port	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez le port HTTP Nomad. La valeur par défaut est 4646.
-NomadRpcPort -nrp	nomad_rpc_port	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez le port RPC Nomad. La valeur par défaut est 4647.
-NomadServerDir -nsd	nomad_server_dir	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez le répertoire du serveur Nomad. Par exemple, la valeur par défaut est <code>\$ClusterCustomDir/nomad/nomadserver</code>
-NomadClientDir -ncd	nomad_client_dir	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez le répertoire du client Nomad. Par exemple, la valeur par défaut est <code>\$ClusterCustomDir/nomad/nomadclient</code>
-NomadCustomOptions -nco	nomad_custom_options	Facultatif. Spécifiez les valeurs des options en les séparant par des virgules et en mettant entre guillemets toute valeur qui contient une virgule. Format requis : [Nom Option=ValeurOption]
-ZookeeperHosts -zh	zookeeper_hosts	Spécifiez les hôtes Zookeeper à l'aide de valeurs séparées par des virgules.
-ZookeeperPort -zp	zookeeper_port	Spécifiez le port Zookeeper. La valeur par défaut est 2181.
-ZookeeperPeerPort -zpp	zookeeper_peer_port	Spécifiez le port d'homologue Zookeeper. La valeur par défaut est 2888.
-ZookeeperLeaderPort -zlp	zookeeper_leader_port	Spécifiez le port leader Zookeeper. La valeur par défaut est 3888.

Option	Argument	Description
-ZookeeperInstallDir -zih	zookeeper_install_dir	Spécifiez le répertoire d'installation de Zookeeper : (la valeur par défaut est <code>\$ClusterCustomDir/zk/install</code>)
-ZookeeperDataDir -zdd	zookeeper_data_dir	Spécifiez le répertoire de données de Zookeeper : (la valeur par défaut est <code>\$ClusterCustomDir/zk/data</code>)
-ZookeeperCustomOptions -zco	zookeeper_custom_options	Facultatif. Options personnalisées de Zookeeper, séparées par des virgules. Spécifiez chaque option au format suivant : [OptionName=OptionValue] Mettez entre guillemets doubles les valeurs des options qui contiennent une virgule.
-SolrHosts -sh	solr_hosts	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez les hôtes Solr.
-SolrPort -sop	solr_port	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez le port Solr. La valeur par défaut est 8983.
-SolrInstallDir -sih	solr_install_dir	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez le répertoire d'installation Solr. La valeur par défaut est <code>\$ClusterCustomDir/solr/install</code> .
-SolrDataDir -sdd	solr_data_dir	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez le répertoire de données Solr. La valeur par défaut est <code>\$ClusterCustomDir/solr/data</code>
-SolrCustomOptions -sco	solr_custom_options	Facultatif. Spécifiez les options personnalisées de Solr. Spécifiez les options au format suivant : [OptionName=OptionValue]. Les options multiples peuvent être séparées par une virgule. Spécifiez la valeur des options, en mettant entre guillemets doubles toute valeur qui contient une virgule.

Option	Argument	Description
-MongoHosts -mdh	mongo_db_hosts	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez les hôtes MongoDB.
-MongoPort -mdp	mongo_port	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez le port MongoDB. Le numéro de port par défaut est 27017.
-MongoLogDir -mdl	mongo_log_dir	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez le répertoire de journalisation MongoDB. La valeur par défaut est <code>\$ClusterCustomDir/mongo/log</code>
-MongoDataDir -mdd	mongo_data_dir	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez le répertoire de données MongoDB. Le répertoire par défaut est <code>\$ClusterCustomDir/mongo/data</code>
-MongoCustomOptions -mco	mongo_custom_options	Facultatif. Spécifiez les options personnalisées de MongoDB. Spécifiez les options personnalisées au format suivant : <code>[OptionName=OptionValue]</code> . Séparez les options multiples par une virgule. Spécifiez la valeur des options, en mettant entre guillemets doubles toute valeur qui contient une virgule.
-PostgresHost -pgh	postgres_host	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez l'hôte Postgres.
-PostgresPort -pgp	postgres_port	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez le port Postgres. Le numéro de port par défaut est 5432.
-PostgresInstallationDir -pgdir	postgres_installation_dir	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez le répertoire d'installation Postgres. Le répertoire par défaut est <code>\$ClusterCustomDir/postgres/install</code> .

Option	Argument	Description
-PostgresLogDir -pgldir	postgres_log_dir	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez le répertoire de journalisation Postgres. Le répertoire par défaut est \$ClusterCustomDir/postgres/log.
-PostgresDataDir -pgddir	postgres_data_dir	Obligatoire si vous activez la propriété de configuration avancée "-eadvc" en la définissant sur true. Spécifiez le répertoire de données Postgres. Le répertoire par défaut est \$ClusterCustomDir/postgres/data.
-PostgresCustomOptions -pgco	postgres_custom_options	Facultatif. Spécifiez les options personnalisées de Postgres. Spécifiez les options personnalisées au format suivant : [OptionName=OptionValue]. Les options multiples peuvent être séparées par une virgule. Spécifiez la valeur des options, en mettant entre guillemets doubles toute valeur qui contient une virgule.
-ElasticHosts -esh	elastic_hosts	Spécifiez le nom d'hôte elastic de la machine sur laquelle Elasticsearch est installé. Vous pouvez entrer plusieurs noms d'hôte séparés par des virgules.
-ElasticHttpPort -eshp	elastic_httpport	Spécifiez le numéro de port d'Elasticsearch que Data Privacy Management utilise pour se connecter à l'interface utilisateur Web d'Elasticsearch. La valeur par défaut est 9200.
-ElasticTcpPort -estp	elastic_tcpport	Spécifiez le numéro de port d'Elasticsearch que Data Privacy Management utilise pour se connecter à l'application Elasticsearch. La valeur par défaut est 9300.
-ElasticLogDir -esld	elastic_log_dir	Spécifiez le répertoire de journalisation elastic. Emplacement de stockage des fichiers journaux d'Elasticsearch. La valeur par défaut est /var/log/elasticsearch.

Option	Argument	Description
-ElasticDataDir -esdd	elastic_data_dir	Spécifiez le répertoire de données elastic. Emplacement de stockage des données de Data Privacy Management dans Elasticsearch. La valeur par défaut est <code>/var/lib/elasticsearch</code> .
-ElasticClusterName -escn	elastic_cluster_name	Spécifiez le nom du cluster Elasticsearch.
-ElasticEnableTls -etls	elastic_enable_Tls	Sélectionnez l'option permettant d'activer le protocole TLS (Transport Layer Security) pour le service. La valeur par défaut est False.
-ElasticUserName -eun	elastic_user_name	Spécifiez le nom d'utilisateur SSL d'Elasticsearch.
-ElasticPassword -epswd	elastic_password	Spécifiez le mot de passe SSL d'Elasticsearch.
-SparkMasterNode -smn	spark_master_node	Spécifiez le nom du nœud principal Spark. Il doit s'agir du nœud de passerelle du service de cluster Informatique.
-SparkMasterPort -smp	spark_master_port	Spécifiez le numéro de port que Data Privacy Management utilise pour se connecter au nœud principal Spark.
-SparkSlaveNodes -ssn	spark_slave_nodes	Spécifiez les nœuds esclaves Spark. Ceux-ci se trouvent généralement sur les nœuds de traitement. Il peut s'agir de plusieurs valeurs séparées par des virgules.
-SparkExecutorCores -sec	spark_executor_cores	Nombre de noyaux d'exécuteur Spark utilisés.
-SparkLogDir -sld	spark_log_dir	Spécifiez le répertoire de journalisation Spark. Emplacement de stockage des fichiers journaux de Spark. La valeur par défaut est <code>/var/log/spark</code> .
-DPMEnable -dpme	dpm_enable	Activez l'activité utilisateur utilisée par les services de cluster Informatique. La valeur par défaut est False.

Option	Argument	Description
-DPMEnableAdvanceConfig -dpmeadv	dpm_enable_advance_config	Configurez les propriétés des applications et des services associés de DPM. La valeur par défaut est False.
-EnableAdvanceConfig -eadvc	enable_advance_config	Configurez les propriétés des applications et des services associés. La valeur par défaut est False.

ListServiceOptions

Répertorie les options pour le service de cluster Informatica.

La syntaxe de la commande infacmd ics ListServiceOptions est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd ics ListServiceOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de cluster Informatica.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

ListServiceProcessOptions

Répertorie les options de processus pour le service de cluster Informatica.

La syntaxe de la commande infacmd ics ListServiceProcessOptions est la suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd ics`
`ListServiceProcessOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de cluster Informatica.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-NodeName -nn	node_name	Obligatoire. Nom du nœud d'exécution du processus de service.

shutdownCluster

Arrête le service de cluster Informatica et les services correspondants, tels que Nomad, Solr, MongoDB et Postgres SQL.

La syntaxe de la commande `infacmd.sh ics shutdownCluster` est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd.sh ics shutdownCluster` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Fait référence au nom du service de cluster Informatica.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

UpdateServiceOptions

Met à jour les options du service de cluster Informatica. Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

La syntaxe de la commande infacmd ics UpdateServiceOptions est la suivante :

```
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,...]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd ics UpdateServiceOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de cluster Informatica.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Options -o	options	Obligatoire. Entrez la paire nom-valeur séparée par des espaces.

Option	Argument	Description
-PrimaryNode -nn	node_name	Facultatif. Nœud principal sur lequel le service de cluster Informatica s'exécute.
-BackupNodes -bn	node_name1,node_name2,...	Facultatif. Nœuds sur lesquels le service de cluster Informatica peut s'exécuter si le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.

UpdateServiceProcessOptions

Met à jour les options du processus de service de cluster Informatica. Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

La syntaxe de la commande `infacmd ics UpdateServiceProcessOptions` est la suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd ics UpdateServiceProcessOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-NodeName -nn	node_name	Obligatoire. Nom du nœud d'exécution du processus de service.

Option	Argument	Description
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de cluster Informatica.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Options -o	options	Obligatoire. Entrez la paire nom-valeur séparée par des espaces.

CHAPITRE 20

Référence de commande infacmd ipc

Ce chapitre comprend les rubriques suivantes :

- [ExportToPC, 342](#)
- [ImportFromPC, 346](#)
- [genReuseReportFromPC, 348](#)

ExportToPC

Exporte les objets depuis le référentiel modèle ou un fichier d'exportation et les convertit en objets PowerCenter.

La commande ExportToPC convertit des objets depuis le référentiel modèle ou depuis un fichier XML que vous avez exporté depuis le référentiel modèle. Vous devez choisir soit un référentiel modèle soit un fichier source pour l'exportation. Si vous choisissez les deux options, l'option du fichier source est prioritaire. Exécutez la commande ExportToPC pour créer un fichier XML que vous pouvez importer dans PowerCenter avec le programme pmrep.

La commande infacmd ipc ExportToPC utilise la syntaxe suivante :

```
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]

Le tableau suivant décrit les options et arguments de la commande infacmd ipc ExportToPC :

Option	Argument	Description
-Release -rel	release_number	Requis. Numéro de version de PowerCenter.
-SourceFile -sf	source_file	Facultatif. Chemin d'accès complet à un fichier XML contenant les objets source que vous avez exporté avec l'outil Developer tool.

Option	Argument	Description
-SourceRepository -sr	source_repository	<p>Facultatif. Référentiel modèle qui contient les objets à exporter vers PowerCenter.</p> <p>Pour spécifier l'hôte et le port de passerelle pour la connexion au service de référentiel modèle, utilisez la syntaxe de commande suivante dans un domaine non-Kerberos :</p> <pre><Model repository name>@<host>:<port>#<projectname> ? user=<username>[&namespace=<namespace>]&password=<password></pre> <p>Pour spécifier le nom de domaine lorsqu'il existe plusieurs nœuds de passerelle, utilisez la syntaxe de commande suivante pour établir une connexion résiliente au service de référentiel modèle dans un domaine non-Kerberos :</p> <pre><Model repository name>@<domainname>#<projectname> ? user=<username>[&namespace=<namespace>]&password=<password></pre> <p>Pour spécifier le nom de domaine avec les informations d'identification connectées, utilisez la syntaxe de commande suivante pour exécuter la commande avec l'authentification unique :</p> <pre><Model repository name>@<domainname>#<projectname> ?isloggedinuser=true[&namespace=<namespace>]</pre> <p>Pour spécifier l'hôte et le port de passerelle avec les informations d'identification connectées, utilisez la syntaxe de commande suivante pour exécuter la commande avec l'authentification unique :</p> <pre><Model repository name>@<host>:<port>#<projectname> ?isloggedinuser=true[&namespace=<namespace>]</pre> <p>Pour spécifier l'hôte et le port de passerelle avec les informations d'identification de l'utilisateur que vous indiquez à la place des informations d'identification connectées, utilisez la syntaxe de commande suivante dans un domaine Kerberos :</p> <pre><Model repository name>@<host>:<port>#<projectname> ? iskerberos=true&user=<username>[&namespace=<namespace>]&password=<password> &Kerberosrealm=<kerberosrealm></pre> <p>Pour spécifier le nom de domaine avec les informations d'identification de l'utilisateur que vous indiquez à la place des informations d'identification connectées, utilisez la syntaxe de commande suivante dans un domaine Kerberos :</p> <pre><Model repository name>@<domainname>#<projectname> ? iskerberos=true&user=<username>[&namespace=<namespace>]&password=<password> &Kerberosrealm=<kerberosrealm></pre> <p>Le paramètre de port est le port HTTP. Le paramètre &namespace est facultatif. L'espace de noms par défaut est natif.</p>
-SourceFolders -f	source_folders	<p>Si vous utilisez -sr, vous devez utiliser -f ou -so.</p> <p>Liste des dossiers source que vous voulez exporter dans le référentiel modèle. Vous pouvez exporter des mapplets, des mappages et des modèles d'objets de données logiques depuis les dossiers source vers PowerCenter. Si vous exportez plus d'un objet, vous devez séparer chaque objet dans la liste avec un espace.</p>

Option	Argument	Description
SourceObjects -so	source_objects	<p>Si vous utilisez -sr, vous devez utiliser -f ou -so.</p> <p>Liste des objets source que vous voulez exporter dans le référentiel modèle. Vous pouvez exporter des mapplets, des mappages et des modèles d'objets de données logiques vers PowerCenter. Vous pouvez décrire l'objet sous la forme d'un nom.</p> <p>Utilisez la syntaxe suivante :</p> <pre>name=/<path>/<objectname> [&type=<typename>]</pre> <p>Vous devez inclure le chemin d'accès complet de l'objet. Si vous exportez plus d'un objet, vous devez séparer chaque objet dans la liste avec un espace.</p> <p>Vous pouvez entrer les types suivants :</p> <ul style="list-style-type: none"> - Mappage. Sert à exporter le mappage et des mapplets. - DataObjectModel. Sert à exporter des modèles d'objets de données logiques. <p>Le type n'est pas sensible à la casse. La valeur par défaut est le mappage.</p>
-Recursive -r	-	<p>Facultatif. Exporte tous les mappages et modèles d'objets de données logiques depuis les dossiers source. Exporte chaque sous-dossier au-dessous des objets et tous les sous-dossiers en dessous.</p> <p>La valeur par défaut est False.</p>
-TargetLocation -tl	target_location	Facultatif. Chemin d'accès complet pour le fichier XML cible.
-TargetFolder -tf	target_folder_name	Facultatif. Dossier PowerCenter pour y exporter les objets. La commande ExportToPC place le nom de dossier dans le fichier XML cible. Si vous ne configurez pas un nom de dossier, la commande ExportToPC crée un nom de dossier.
-CodePage -cp	target_code_page	Facultatif. Page de code du référentiel PowerCenter. La valeur par défaut est UTF-8.
-Check -c	-	<p>Facultatif. Teste la conversion sans créer de fichier cible.</p> <p>La valeur par défaut est False.</p>
-ReferenceDataLocation -rdl	reference_data_output_location	Facultatif. Emplacement où vous souhaitez enregistrer les données de la table de référence. L'outil Developer enregistre les données de table de référence sous un ou plusieurs fichiers .dic de dictionnaire.
-ConvertMappletTargets -cmt	-	<p>Facultatif. Convertit les cibles dans les mapplets en transformations de sortie dans le mapplet PowerCenter.</p> <p>Les mapplets PowerCenter ne peuvent pas contenir de cibles. Si l'exportation comprend un mapplet qui contient une cible et que vous ne sélectionnez pas cette option, le processus d'exportation échoue.</p> <p>La valeur par défaut est False.</p>
-ConvertMappingstoMapplets -cmm	-	<p>Facultatif. Convertit des mappages de l'outil Developer tool en mapplets PowerCenter. L'outil Developer tool convertit les sources et cibles présentes dans les mappages en transformations d'entrée et de sortie dans un mapplet PowerCenter.</p> <p>La valeur par défaut est False.</p>

Option	Argument	Description
-NoValidation -nv	-	Facultatif. La commande ExportToPC ne valide pas les objets source avant leur conversion. La valeur par défaut est False.
-DSTErrorFormat -def	-	Facultatif. Les messages d'erreur s'affichent dans un format que l'outil Developer tool peut analyser. Le chemin d'accès complet de chaque objet s'affiche dans les messages d'erreur. La valeur par défaut est l'affichage des erreurs dans un format convivial.
OptimizationLevel - 0	optimization_level	Facultatif. Contrôle les méthodes d'optimisation que le service d'intégration de données applique au mappage. Entrez la valeur numérique associée au niveau d'optimisation que vous voulez configurer. Entrez l'une des valeurs numériques suivantes : <ul style="list-style-type: none"> - 0 (aucun). Le service d'intégration de données n'applique aucune optimisation. - 1 (minimum). Le service d'intégration de données applique la méthode d'optimisation de projection précoce. - 2 (normal). Le service d'intégration de données applique les méthodes d'optimisation de projection précoce, de sélection précoce, de nettoyage de branche, push-into, de refoulement et de prédicat. Le niveau d'optimisation par défaut est Normal. - 3 (complet). Le service d'intégration de données applique les méthodes d'optimisation basée sur le coût, de projection précoce, de sélection précoce, de nettoyage de branche, de prédicat, push-into, de refoulement et de semi-jointure. <p>Si vous n'utilisez pas cette option, le service d'intégration de données applique le niveau d'optimisation configuré dans les propriétés de mappage de l'application déployée dans l'outil Administrator tool.</p>

ImportFromPC

Convertit un fichier XML d'objet du référentiel PowerCenter en un fichier XML d'objet du référentiel modèle. Exportez les objets du référentiel PowerCenter dans un fichier XML. Exécutez la commande importFromPC pour créer un fichier XML cible avec les objets que vous pouvez importer dans un référentiel modèle.

Vous pouvez importer le fichier cible XML dans un référentiel modèle à l'aide de la commande infacmd tools ImportObjects ou à partir de l'outil Developer tool. Si vous utilisez la ligne de commande pour importer la cible du fichier XML, ImportFromPC n'affecte pas les connexions pour les objets du référentiel modèle dans la cible du fichier XML. Vous pouvez attribuer des connexions à l'aide de la commande infacmd oie ImportObjects ou à partir de l'outil Developer tool.

La commande infacmd ipc importFromPC utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande infacmd ipc ImportFromPC :

Option	Argument	Description
-Release -rel	release_number	Requis. Version du référentiel modèle.
-SourceFile -sf	source_file	Requis. Chemin complet d'un fichier XML PowerCenter contenant les objets source.
-TargetFile -tf	target_location	Requis si vous ne spécifiez pas -Check ni -c. Chemin complet vers un fichier XML cible.
-Check -c	-	Facultatif. Teste la conversion sans créer de fichier cible. Lorsque vous testez la conversion de l'objet, vous ne nécessitez pas d'emplacement cible.
-Db2Type -dt	default_db2_type	Facultatif. Type de sous-système DB2 utilisé pour la conversion. Vous pouvez spécifier Db2Type, Db2TypesFile ou les deux. Si vous spécifiez Db2Type et Db2TypesFile pour les objets IBM DB2, la source et la cible DB2 qui ne sont pas répertoriées dans Db2TypesFile sont converties en Db2Type. Si vous ne spécifiez pas de type de sous-système DB2, le type par défaut est utilisé. La valeur par défaut est LUW.
-Db2TypesFile -df	db2_types_file	Facultatif. Fichier de propriétés qui contient la source DB2 de PowerCenter et le type de sous-système Db2. Vous pouvez utiliser un type de fichier Db2 si la source et la cible Db2 proviennent de sous-systèmes différents tels que LUW, z/OS ou i/OS. Vous pouvez spécifier Db2Type, Db2TypesFile ou les deux. Si vous spécifiez Db2Type et Db2TypesFile pour les objets IBM DB2, la source et la cible DB2 qui ne sont pas répertoriées dans Db2TypesFile sont converties en Db2Type. Si vous ne spécifiez pas le type de sous-système DB2, le type par défaut est utilisé. La valeur par défaut est LUW.
-DefaultLookupConType -dl	default_lookup_con_type	Facultatif. Type de connexion de recherche utilisé pour la conversion. Vous pouvez spécifier DefaultLookupConType ou LookupConTypesFile ou les deux. Si vous spécifiez DefaultLookupConType et LookupConTypesFile pour les objets de recherche, les transformations Recherche qui ne sont pas répertoriées dans LookupConTypesFile sont converties en DefaultLookupConType. Si vous ne spécifiez pas DefaultLookupConType pour un objet de recherche lors de la conversion, le type de connexion par défaut est utilisé. La valeur par défaut est ODBC.

Option	Argument	Description
- LookUpConTypesFile -lcf	lookup_connection_type_file	Facultatif. Fichier de propriétés qui contient la source et le type de connexion de la recherche. Vous pouvez utiliser un fichier de type de connexion de recherche si les objets de recherche proviennent de différentes bases de données, comme Oracle ou IBM DB2. Vous pouvez spécifier DefaultLookUpConType ou LookUpConTypesFile, ou les deux. Si vous spécifiez les deux fichiers pour les objets de recherche, les transformations Recherche qui ne sont pas répertoriées dans LookUpConTypesFile sont converties en DefaultLookUpConType. Si vous ne spécifiez pas DefaultLookUpConType pour un objet de recherche lors de la conversion, le type de connexion par défaut est utilisé. La valeur par défaut est ODBC.
- ConvertOverrideproperties -orprops	True False	Facultatif. Préserve les propriétés remplacées pour une source, une cible et des transformations PowerCenter réutilisables pendant la conversion. La commande crée des transformations non réutilisables pour les transformations PowerCenter avec des propriétés de remplacement. Elle crée également des objets de données réutilisables pour les sources et les cibles PowerCenter avec des propriétés de remplacement. Les valeurs valides sont True ou False. La valeur par défaut est True.
-LogFile -lf	log_file	Facultatif. Chemin et nom du fichier journal de sortie. La valeur par défaut est STDOUT.

genReuseReportFromPC

Génère un rapport qui évalue le nombre de mappages PowerCenter pouvant être réutilisés dans le référentiel modèle d'un environnement natif et Hadoop. Vous pouvez générer le rapport sous la forme d'un fichier PDF ou Excel.

Remarque: Si vous générez le rapport sous la forme d'un fichier Excel, cliquez sur **Activer le contenu** dans la barre de message pour charger toutes les feuilles.

Avant d'exécuter la commande `infacmd ipc genReuseReportFromPC`, effectuez les tâches suivantes :

- Configurez les variables d'environnement requises pour la commande `pmrep`.
- Dans un environnement Linux, accordez les autorisations de lecture, d'écriture et d'exécution sur chaque dossier de version situé dans le répertoire suivant : <répertoire d'installation du serveur Informatica>/tools/pcutils

La syntaxe de la commande `infacmd ipc genReuseReportFromPC` est la suivante :

```
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]

```

Le tableau suivant décrit les options et les arguments de la commande `infacmd ipc genReuseReportFromPC` :

Option	Argument	Description
-RepositoryName -r	Pc_Repository_Name	Requis. Nom du référentiel PowerCenter.
-HostName -h	Pc_Domain_HostName	Requis. Nom d'hôte du référentiel PowerCenter.
-PortNumber -o	Pc_Domain_PortNumber	Requis. Numéro de port du nœud de passerelle.
-UserName -n	Domain_Username	Facultatif. Nom d'utilisateur du domaine PowerCenter. Si vous n'entrez pas un nom d'utilisateur, la commande utilise la valeur de la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> .
Password -x	Domain_Password	Facultatif. Mot de passe du domaine PowerCenter. Si vous n'entrez aucun nom d'utilisateur, la commande utilise la valeur de la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> .
-SecurityDomain -s	Pc_Repository_Security_domain	Requis si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Si vous ne spécifiez aucun domaine de sécurité, la commande utilise la valeur de la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Vous pouvez spécifier la valeur Natif, LDAP ou SSO. La valeur par défaut est Natif.
-folderNames -f	Pc_Folder_Names	Requis. Dossiers PowerCenter qui contiennent les objets à réutiliser. Les noms de dossier peuvent contenir des expressions ou des caractères spéciaux * comme expressions. Remarque: Dans un environnement Linux, vous ne pouvez pas utiliser le caractère \$ dans le nom de dossier.

Option	Argument	Description
-SrcRelease -srel	Pc_Release_version	Requis. Version associée au référentiel PowerCenter. Entrez la version au format suivant : 10.x.x Par exemple, entrez une version au format suivant : 10.2.0
-targetRelease -trel	Target_Release_version	Facultatif. Version associée au référentiel modèle. Si vous ne spécifiez pas une version, la commande utilise la version du produit. Vous pouvez entrer une version à partir de la version 10.0.0. Entrez la version au format suivant : 10.x.x Par exemple, entrez une version au format suivant : 10.2.1
-CodePage -cp	Pc_Repository_code_page	Facultatif. Page de code du référentiel PowerCenter. La valeur par défaut est UTF-8.
-targetDir -td	Target_Directory	Requis. Emplacement du répertoire cible sur la machine sur laquelle le client et le serveur infacmd sont exécutés. Vous devez disposer des autorisations de lecture, d'écriture et d'exécution sur le répertoire cible. Par exemple, entrez l'emplacement du client infacmd au format suivant : installed_location_of_client\clients\DeveloperClient\infacmd Par exemple, entrez l'emplacement du serveur infacmd au format suivant : installed_location_of_server\isp\bin Remarque: Sur une machine Linux, vous ne pouvez pas utiliser le caractère \$ dans le nom du répertoire cible.
authenticationType -at	authentication_Type	Requis. Type d'authentification utilisateur pour le domaine. Entrez l'une des valeurs suivantes : LDAP, Natif ou Connexion unique Kerberos.
-LogFile -lf	Log_file_Name	Facultatif. Nom du fichier journal généré. Si vous ne spécifiez aucun nom, la commande imprime les journaux dans la console. Utilisez la valeur chemin_fichier/nom_fichier. Si vous entrez un nom de fichier, un fichier journal portant le même nom s'affiche dans le dossier infacmd. Si vous entrez un chemin de répertoire non valide, un fichier journal portant le nom de chemin s'affiche dans le dossier infacmd. Par exemple, si vous entrez x comme chemin de répertoire, un fichier journal nommé x s'affiche dans le dossier.
-Font	Font_to_use_for_PDF	Facultatif. Emplacement du fichier de police permettant d'avoir des caractères Unicode dans le rapport.

Option	Argument	Description
- ExecutionEnvironment -execMode	Execution_Environment	Facultatif. Moteur d'exécution dans l'environnement Hadoop. Le rapport valide les mappages en fonction du moteur d'exécution que vous choisissez. Vous pouvez utiliser Blaze ou Spark comme valeur. Si vous n'entrez pas de valeur, le rapport s'exécutera par rapport à tous les moteurs et n'inclura que le moteur comportant le moins d'erreurs.
-BlockSize	Block_Size	Facultatif. Nombre de mappages sur lesquels vous souhaitez exécuter la commande <code>infacmd ipc genReuseReportFromPC</code> . Si vous n'entrez pas de valeur, le rapport exécute et convertit tous les mappages contenus dans chaque dossier à la fois. Lorsque la mémoire requise pour l'exécution de la commande n'est pas disponible, utilisez l'option <code>-BlockSize</code> pour contrôler le nombre de mappages au lieu d'exécuter la commande sur tous les mappages dans le référentiel.

CHAPITRE 21

Référence de commande infacmd isp

Le programme infacmd isp administre le domaine Informatica, la sécurité et les services d'applications de PowerCenter. Vous pouvez activer et désactiver les services Informatica avec les commandes infacmd isp.

Ce chapitre comprend les commandes que vous pouvez utiliser avec le programme infacmd isp.

AddAlertUser

Abonne un utilisateur à des courriels de notifications d'alertes. Avant de pouvoir abonner des utilisateurs à des alertes, vous devez configurer les paramètres SMTP pour le serveur de messagerie sortante. Vous pouvez exécuter infacmd isp AddAlertUser pour un utilisateur.

Lorsque vous vous abonnez à des alertes, vous recevez des courriels de notification de domaine et de service pour les objets pour lesquels vous disposez d'une autorisation.

La commande infacmd isp AddAlertUser utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp AddAlertUser :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-AlertUser -au	user_name	Obligatoire. Nom de l'utilisateur que vous souhaitez abonner aux alertes.

LIENS CONNEXES :

- [“UpdateSMTPOptions” à la page 784](#)

AddConnectionPermissions

Assigne des autorisations de connexion à un utilisateur ou un groupe.

La commande infacmd isp AddConnectionPermissions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp AddConnectionPermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-RecipientUserName -run	recipient_user_name	Obligatoire si vous ne spécifiez pas le nom du groupe destinataire. Nom de l'utilisateur auquel l'autorisation de connexion est attribuée.
-RecipientGroupName -rgn	recipient_group_name	Obligatoire si vous ne spécifiez pas le nom d'utilisateur du destinataire. Nom du groupe auquel l'autorisation de connexion est attribuée.
-RecipientSecurityDomain -rsd	recipient_security_domain_name	Obligatoire si le destinataire appartient à un domaine de sécurité LDAP. Nom du domaine de sécurité auquel appartient le destinataire. La valeur par défaut est Natif.

Option	Argument	Description
-ConnectionName -cn	connection_name_security_domain	Requis. Nom de la connexion
-Permission -p	autorisation	Requis. Type d'autorisation à attribuer. Entrez une ou plusieurs des valeurs suivantes, séparées par des espaces : <ul style="list-style-type: none"> - READ - WRITE. Lecture et écriture - EXECUTE - GRANT. Lecture et accord - ALL. Lecture, Écriture, Exécution, Accorder

addCustomLDAPType

Ajoute un type LDAP personnalisé qui définit un service d'annuaire LDAP à partir duquel vous importez des utilisateurs dans un domaine de sécurité LDAP.

La commande `infacmd isp addCustomLDAPType` utilise la syntaxe suivante :

```
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]
```


Le tableau suivant décrit les options et les arguments de la commande `infacmd isp addCustomLDAPType` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-CustomLDAPTypeName -lt	custom_LDAP_type_name	Obligatoire. Nom du type LDAP personnalisé.
-DisplayName -dnpn	display_name	Obligatoire. Nom du type LDAP personnalisé affiché dans l'outil Administrator tool.
-Uid	uid	Obligatoire. Nom de l'attribut dans le service d'annuaire LDAP qui contient l'identificateur unique (UID) que le gestionnaire de service utilise pour identifier les utilisateurs.
-GroupMembershipAttr -gm	group_membership_attr	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient les informations d'appartenance au groupe d'un utilisateur.
-GroupDescriptionAttr -gd	group_description_attr	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient un texte descriptif sur les groupes dans le service d'annuaire.
-UserSurnameAttr -usn	user_surname_attr	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient le nom d'un utilisateur.
-UserGivenNameAttr -ugn	user_given_name_attr	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient le prénom d'un utilisateur.
-GroupMembershipAttr -gm	LDAP_Group_Membership_Attribute	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient les noms des groupes dans le service d'annuaire.
--UserEmailAttr -ue	user_email_attr	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient l'adresse e-mail d'un utilisateur.
-UserEnableAttr -uen	user_enable_attr	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient
-UserTelephoneAttr -utn	user_telephone_attr	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient le numéro de téléphone d'un utilisateur.
-UserDescriptionAttr -ud	user_description_attr	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient la description d'un utilisateur.

Option	Argument	Description
-CN	cn	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient l'attribut qui comprend le nom complet ou le nom commun d'un utilisateur.
- FetchRangedAttr -fr	fetch_ranged_attr	Facultatif. Définissez cette option sur True pour récupérer toutes les valeurs contenues dans les attributs à valeurs multiples. Utilisez cette option uniquement avec Microsoft Active Directory.

AddDomainLink

Ajoute un lien au domaine. enregistre les propriétés de la connexion dans un domaine distant ou lié pour que vous puissiez échanger des métadonnées du référentiel entre le domaine local et le domaine lié.

Vous devriez peut-être ajouter un lien vers un domaine si vous devez accéder à un service de référentiel PowerCenter dans ce domaine.

Vous pouvez ajouter un lien vers un autre domaine Informatica lorsque vous enregistrez ou annulez un référentiel local avec un référentiel global dans un autre domaine Informatica.

La commande `infacmd isp AddDomainLink` utilise la syntaxe suivante :

```
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...
```

Le tableau suivant décrit les options et arguments d'infacmd isp AddDomainLink :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine local.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine local. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-LinkedDomainName -ld	linked_domain_name	Obligatoire. Nom du domaine avec lequel vous souhaitez établir une connexion.
-DomainLink -dl	gateway_host1:port gateway_host2:port...	Obligatoire. Noms d'hôte et numéros de ports pour les nœuds de passerelle du domaine lié.

AddDomainNode

Ajoute un nœud au domaine. Avant de pouvoir démarrer le nœud, vous devez le définir en exécutant DefineGatewayNode ou DefineWorkerNode de la commande infasetup sur le nœud.

La commande infacmd isp AddDomainNode utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp AddDomainNode :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NodeName -nn	node_name	Requis. Nom du nœud que vous souhaitez ajouter au domaine.

Option	Argument	Description
-FolderPath -fp	full_folder_path	Facultatif. Chemin d'accès complet, sans le nom de domaine, du dossier dans lequel vous souhaitez ajouter le nœud. Doit être au format suivant : <i>/parent_folder/child_folder</i> La valeur par défaut est « / » (le domaine).
-EnableServiceRole -esr	True False	Facultatif. Active le rôle de service sur le nœud. Si la valeur est True, les services d'application peuvent s'exécuter sur le nœud. Si la valeur est False, les services d'application ne peuvent pas s'exécuter sur le nœud. Définissez cette valeur sur False uniquement si le nœud est attribué à une grille du service d'intégration de données si vous souhaitez le dédier à l'exécution de mappages. La valeur par défaut est True.
-EnableComputeRole -esr	True False	Facultatif. Active le rôle de calcul sur le nœud. Si la valeur est True, le nœud peut effectuer des calculs demandés par des services d'application distants. Si la valeur est False, le nœud ne peut pas effectuer de calculs demandés par des services d'application distants. Un nœud doit être doté du rôle de calcul si le service d'intégration de données y exécute des tâches. Si le service d'intégration de données n'exécute pas de tâches sur le nœud, vous pouvez désactiver le rôle de calcul. Cependant, l'activation et la désactivation du rôle de calcul n'ont aucun impact sur les performances. La valeur par défaut est True.

AddGroupPrivilege

Assigne un privilège à un groupe dans le domaine. Vous pouvez assigner des privilèges à un groupe pour le domaine. Vous pouvez également assigner des privilèges de groupes pour chaque service d'application dans le domaine.

La commande infacmd isp AddGroupPrivilege utilise la syntaxe suivante :

```
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

Le tableau suivant décrit les options et arguments d'infacmd isp AddGroupPrivilege :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Les noms d'hôte et les numéros de ports pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-GroupName -gn	group_name	Obligatoire. Nom du groupe auquel vous assignez le privilège. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez le nom entre guillemets.

Option	Argument	Description
-GroupSecurityDomain -gsf	group_security_domain	Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient le groupe auquel vous assignez le privilège. La valeur par défaut est Natif.
-ServiceName -sn	service_name	Obligatoire. Nom de service du domaine ou de l'application dont vous voulez afficher les privilèges.
-PrivilegePath -pp	path_of_privilege	Obligatoire. Nom complet du privilège que vous voulez assigner au groupe. Un nom complet inclut le nom du privilège du groupe et le nom du privilège. Par exemple, un nom complet de privilège pour le service de référentiel est dossier/créer. Si le nom du privilège comprend des espaces, placez le chemin entre guillemets comme suit : "Runtime Objects/Monitor/Execute/Manage Execution" Si le nom du privilège inclut le caractère spécial « / », ajoutez le caractère d'échappement « \ » devant, comme suit : "Model/View Model/Export\Import Models"

addLDAPConnectivity

Configure une connexion à un serveur LDAP. Si vous spécifiez un domaine de sécurité, le gestionnaire de service importe les utilisateurs et les groupes du service d'annuaire LDAP dans le domaine de sécurité.

La commande infacmd isp addLDAPConnectivity utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd isp addLDAPConnectivity` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-LDAPAddress -la	ldap_server_address	Obligatoire. Nom d'hôte et numéro de port de la machine qui héberge le service d'annuaire LDAP. Généralement, le numéro de port du serveur LDAP est le 389. Si le serveur LDAP utilise SSL, le numéro de port du serveur LDAP est le 636.
-LDAPPrincipal -lp	ldap_principal	Facultatif. Nom unique (NU) de l'utilisateur principal. Omettez cette option pour vous connecter comme utilisateur anonyme. Pour plus d'informations, consultez la documentation du service d'annuaire LDAP.
-LDAPCredential -lc	ldap_credential	Facultatif. Mot de passe de l'utilisateur principal. Vous pouvez définir un mot de passe avec l'option -lc ou la variable d'environnement INFA_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -lc est prioritaire. Omettez cette option pour vous connecter comme utilisateur anonyme.
-UseSSL -us	use_ssl	Facultatif. Si vous incluez l'option, le service d'annuaire LDAP utilise le protocole Secure Sockets Layer (SSL).
-TrustLDAPCertificate -tc	trust_ldap_certificate	Facultatif. Si vous incluez l'option, PowerCenter se connecte au serveur LDAP sans vérifier le certificat SSL. Si vous n'incluez pas l'option, PowerCenter vérifie que le certificat SSL est signé par une autorité de certification avant de se connecter au serveur LDAP.
-LDAPType -lt	ldap_types=value	Obligatoire. Type de service d'annuaire LDAP. Les services d'annuaire incluent : <ul style="list-style-type: none"> - MicrosoftActiveDirectory - Microsoft Azure Active Directory - SunJavaSystemDirectory - NovellE-Directory - IBMTivoliDirectory - OpenLDAP - Oracle Directory Server (ODSEE) - Oracle Unified Directory Si vous utilisez un service d'annuaire LDAP personnalisé, spécifiez le nom du service.

Option	Argument	Description
-MaxSecurityDomainSize -ms	Max_Security_Domain_size	Facultatif. Nombre maximal de comptes utilisateur à importer dans un domaine de sécurité. La valeur par défaut est 1 000.
-GroupMembershipAttr -gm	LDAP_Group_Membership_Attribute	Facultatif. Nom de l'attribut qui contient des informations d'appartenance au groupe pour un utilisateur.
-LDAPNotCaseSensitive -lnc	LDAP_Not_Case_Sensitive	Facultatif. Indique que les noms d'utilisateur provenant du service d'annuaire LDAP ne sont pas sensibles à la casse. La valeur par défaut est False.
LDAPHostConfigurationName -lcn	LDAP_host_configuration_name	Obligatoire. Nom de la configuration LDAP.

AddLicense

Ajoute une licence au domaine. Après avoir ajouté une licence, vous pouvez l'assigner à un service d'application à l'aide de la commande AssignLicense. Vous devez assigner une licence à un service avant de pouvoir utiliser ce dernier.

La commande infacmd isp AddLicense utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp AddLicense :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-LicenseName -ln	license_name	Obligatoire. Nom de la licence. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Le nom ne peut pas dépasser 79 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "
-LicenseKeyFile -lf	license_key_file	Obligatoire. Chemin du fichier de clé de licence.
-FolderPath -fp	full_folder_path	Facultatif. Chemin d'accès complet, sans le nom de domaine, du dossier dans lequel vous souhaitez ajouter la licence. Doit être au format suivant : <i>/parent_folder/child_folder</i> La valeur par défaut est « / » (le domaine).

AddNamespace

Crée un domaine de sécurité LDAP et définit les filtres afin de rechercher des utilisateurs ou des groupes dans le service d'annuaire. Crée le domaine de sécurité LDAP si le domaine Informatica utilise l'authentification LDAP ou Kerberos.

La commande infacmd isp AddNamespace utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments d'infacmd isp AddNamespace :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Vous pouvez spécifier une valeur pour -sdn ou utiliser la valeur par défaut selon le mode d'authentification : <ul style="list-style-type: none"> - Requis si le domaine utilise l'authentification LDAP. La valeur par défaut est Natif. Pour travailler avec l'authentification LDAP, vous devez spécifier la valeur pour -sdn. - Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. La valeur par défaut est natif pour l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd essaye d'établir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous ne spécifiez pas la variable d'environnement, la valeur par défaut utilisée est de 180 secondes.
-NameSpace -ns	namespace	Requis. Nom du domaine de sécurité LDAP ou Kerberos que vous voulez ajouter. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Le nom ne peut pas contenir d'espaces ou les caractères spéciaux suivants : , + / < > @ ; \ % ? Le nom ne peut pas dépasser 128 caractères. Le nom peut inclure des espaces ASCII, sauf en première et dernière position. Vous ne pouvez pas utiliser d'autres caractères d'espace.
-UserSearchBase -usb	usersearchbase	Le nom unique (DN) de l'entrée sert de point de départ pour rechercher les noms d'utilisateurs dans le service d'annuaire LDAP. Le service d'annuaire LDAP recherche un objet dans le répertoire selon le chemin d'accès dans le nom unique de l'objet. Par exemple, dans Microsoft Active Directory, le nom unique d'un objet utilisateur peut être cn=UserName,ou=OrganizationalUnit,dc=DomainName. La série des noms uniques relatifs indiqués par dc=DomainName identifie le domaine DNS de l'objet.
-UserFilter -uf	userfilter	Chaîne de requête LDAP qui spécifie les critères de recherche pour rechercher des utilisateurs dans le service d'annuaire. Le filtre peut indiquer les types d'attributs, les valeurs d'assertion et les critères de correspondance. Par exemple : le filtre (objectclass = *) recherche tous les objets. Le filtre (&(objectClass=user) (! (cn=susan))) recherche tous les objets utilisateurs sauf « susan ». Pour plus d'informations sur les filtres de recherche, consultez la documentation du service d'annuaire LDAP.
-GroupSearchBase -gsb	groupsearchbase	Le nom unique (DN) de l'entrée sert de point de départ pour rechercher les noms de groupes dans le service d'annuaire LDAP.
-GroupFilter -gf	groupfilter	Chaîne de requête LDAP qui spécifie les critères de recherche pour les groupes dans le service d'annuaire.
-LDAPHostConfigurationName -lcn	LDAP_host_configuration_name	Obligatoire. Nom de la configuration LDAP associée au domaine de sécurité.

AddNodeResource

Ajoute une ressource personnalisée ou une ressource de répertoire de fichier à un nœud.

Quand un service d'intégration PowerCenter est exécuté sur une grille, l'équilibrage de charge peut utiliser des ressources pour distribuer des tâches Session, Command et Event-wait prédéfinies. Si le service d'intégration PowerCenter est configuré pour vérifier des ressources, l'équilibrage de charge distribue des tâches aux nœuds où les ressources sont ajoutées et activées.

La commande infacmd isp AddNodeResource utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp AddNodeResource :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NodeName -nn	node_name	Requis. Nom du nœud auquel vous souhaitez ajouter une ressource.
-ResourceCategory -rc	resource_category	Facultatif. Catégorie de la ressource. Les catégories valides incluent : - PCIS. Ressource pour le service d'intégration PowerCenter. - DIS. Réserve pour un usage futur. La valeur par défaut est PCIS.
-ResourceType -rt	resource_type	Requis. Type de ressource. Les types valides comprennent : - Personnalisé - Répertoire de fichier
-ResourceName -rn	resource_name	Requis. Nom de la ressource. Le nom ne peut pas dépasser 79 caractères, commencer ou se terminer par des espaces ou contenir des retours chariot, des tabulations ou les caractères suivants : \ / * ? < > " \$
-ResourceValue -rv	resource_value	Facultatif. Réserve pour une utilisation ultérieure.

AddRolePrivilege

Attribue un privilège à un rôle dans le domaine. Vous pouvez attribuer des privilèges à un rôle pour le domaine. Vous pouvez également attribuer des privilèges de rôles pour chaque service d'application dans le domaine.

La commande infacmd isp AddRolePrivilege utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp AddRolePrivilege :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-RoleName -rn	role_name	Requis. Nom du rôle auquel vous attribuez le privilège. Pour entrer un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.

Option	Argument	Description
-ServiceType -st	service_type	Requis. Type de service de domaine ou d'application auquel vous attribuez le privilège pour le rôle. Les types de services comprennent : <ul style="list-style-type: none"> - AS. Service Analyst - CMS. Service de gestion de contenu - CS. Service de catalogue - DIS. Service d'intégration de données - DOMAIN. Domaine - MM. Service Metadata Manager - MRS. Service de référentiel modèle - RS. Service de référentiel PowerCenter - TDM. Service Test Data Manager - TDW. Service Test Data Warehouse - SATS. Service Secure at Source. - SCH. Service de planificateur
-PrivilegePath -pp	path_of_privilege	Requis. Nom complet du privilège que vous souhaitez attribuer au groupe. Un nom complet inclut le nom du groupe de privilèges et le nom du privilège. folder/create constitue par exemple un nom complet de privilège pour le service de référentiel. Si le nom du privilège comprend des espaces, placez le chemin entre guillemets comme suit : "Runtime Objects/Monitor/Execute/Manage Execution" Si le nom du privilège inclut le caractère spécial « / », ajoutez le caractère d'échappement « \ » devant, comme suit : "Model/View Model/Export\Import Models"

AddServiceLevel

Ajoute un niveau de service.

Les niveaux de services établissent un ordre de priorité parmi les tâches qui attendent d'être réparties. Vous pouvez créer différents niveaux de service qu'un développeur de tâche peut assigner à des flux de travail.

Chaque niveau de service que vous créez dispose d'un nom, d'une priorité de répartition, ainsi que d'un temps d'attente de répartition maximal. La priorité de répartition est un nombre qui établit la priorité au moment de la répartition. L'équilibrage de charge répartit les tâches à priorité élevée avant celles dont la priorité est faible. Le délai d'attente maximal de répartition spécifie le nombre de fois que l'équilibrage de charge attendra avant de modifier la priorité de répartition d'une tâche en priorité la plus élevée.

La commande infacmd isp AddServiceLevel utilise la syntaxe suivante :

```
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 ...
```

Le tableau suivant décrit les options et arguments d'infacmd isp AddServiceLevel :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceLevelName -ln	service_level_name	Obligatoire. Nom du niveau de service.
-ServiceLevel -sl	option_name=value	Obligatoire. Propriétés du niveau de service. Vous pouvez définir les propriétés suivantes : <ul style="list-style-type: none"> - DispatchPriority. Priorité initiale de répartition. Les numéros les plus petits ont une priorité plus élevée. La priorité 1 est la plus élevée. La valeur par défaut est 5. - MaxDispatchWaitTime. Délai en secondes qui peut s'écouler avant que l'équilibrage de charge ne modifie la priorité de répartition d'une tâche vers la priorité la plus élevée. La valeur par défaut est 1 800.

AddUserPrivilege

Assigne un privilège à un utilisateur dans le domaine. Vous pouvez assigner des privilèges d'utilisateurs pour chaque application dans le domaine.

La commande infacmd isp AddUserPrivilege utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp AddUserPrivilege :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ExistingUserName -eu	existing_user_name	Obligatoire. Compte utilisateur auquel vous attribuez le privilège. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité de l'utilisateur auquel vous attribuez le privilège. La valeur par défaut est Natif.
-ServiceName -sn	service_name	Obligatoire. Nom de service du domaine ou de l'application dont vous souhaitez afficher les privilèges.
-PrivilegePath -pp	path_of_privilege	Obligatoire. Nom complet du privilège que vous souhaitez attribuer au groupe. Un nom complet inclut le nom du groupe de privilèges et le nom du privilège. folder/create constitue par exemple un nom complet de privilège pour le service de référentiel. Si le nom du privilège comprend des espaces, placez le chemin entre guillemets comme suit : "Runtime Objects/Monitor/Execute/Manage Execution" Si le nom du privilège inclut le caractère spécial « / », faites-le précéder du caractère d'échappement « \ », comme suit : "Model/View Model/Export\ /Import Models"

AddUserToGroup

Ajoute un utilisateur natif ou LDAP à un groupe natif dans le domaine. L'utilisateur hérite de l'ensemble des autorisations et privilèges associés au groupe.

La commande infacmd isp AddUserToGroup utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp AddUserToGroup :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ExistingUserName -eu	existing_user_name	Obligatoire. Nom de l'utilisateur que vous souhaitez ajouter.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur que vous souhaitez ajouter. La valeur par défaut est Natif.
-GroupName -gn	group_name	Obligatoire. Nom du groupe auquel vous souhaitez ajouter l'utilisateur.

AssignDefaultOSProfile

Attribue un profil de système d'exploitation par défaut à un utilisateur ou à un groupe.

La syntaxe de la commande infacmd isp AssignDefaultOSProfile est la suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd isp AssignDefaultOSProfile` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine.
-OSProfileName -on	OSProfile_name	Requis. Nom du profil de système d'exploitation. Le nom du profil de système d'exploitation peut comporter jusqu'à 80 caractères. Il ne peut pas inclure d'espaces ou les caractères spéciaux suivants : % * + \ / ? ; < >
-RecipientName -nm	nom_destinataire	Requis. Nom d'utilisateur ou nom de groupe auquel attribuer le profil de système d'exploitation par défaut.
-RecipientSecurityDomain -ns	domaine_sécurité_destinataire	Requis si vous utilisez une authentification LDAP et que vous attribuez des autorisations d'utilisateur. Nom du domaine de sécurité auquel appartient l'utilisateur.
-RecipientType -ty	type_destinataire	Requis. Indiquez si le profil de système d'exploitation doit être attribué à un utilisateur ou à un groupe. Entrez l'une des valeurs suivantes : - UserIdentity - GroupIdentity

AssignedToLicense

Répertorie les services assignés à une licence. Vous pouvez répertorier les services actuellement assignés à une licence.

La commande `infacmd isp AssignedToLicense` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'`infacmd isp AssignedToLicense` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-LicenseName -ln	license_name	Obligatoire. Nom de la licence.

AssignGroupPermission

Assigne une autorisation de groupe à un objet.

Les autorisations permettent à un groupe d'accéder à des objets dans un domaine. Les objets incluent le domaine, les dossiers, les nœuds, les grilles, les licences et les services d'applications. Par exemple, si vous assignez une autorisation de groupe à un dossier, le groupe hérite de l'autorisation sur tous les objets dans le dossier.

La commande infacmd isp AssignGroupPermission utilise la syntaxe suivante :

```
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

Le tableau suivant décrit les options et arguments d'infacmd isp AssignGroupPermission :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ExistingGroup -eg	existing_group_name	Obligatoire. Nom du groupe auquel vous souhaitez attribuer une autorisation sur un objet.
-GroupSecurityDomain -gsf	group_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité du groupe auquel vous souhaitez attribuer une autorisation. La valeur par défaut est Natif.
-ObjectName -on	object_name	Obligatoire. Nom de l'objet auquel vous souhaitez attribuer l'autorisation d'accès de groupe.
-ObjectType -ot	object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE	Obligatoire. Type d'objet. Entrez l'une des valeurs suivantes : <ul style="list-style-type: none"> - Service - Licence - Nœud - Grille - Dossier - OSProfile

AssignISToMMService

Assigne le service d'intégration PowerCenter associé à un service de gestionnaire de métadonnées.

La commande infacmd isp AssignISToMMService utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et arguments d'infacmd isp AssignISToMMService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Obligatoire. Nom du service de gestionnaire de métadonnées auquel vous voulez assigner le service d'intégration.
-IntegrationService -is	integration_service_name	Obligatoire. Nom du service d'intégration PowerCenter que vous souhaitez associer au service Metadata Manager.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Obligatoire si le domaine utilise l'authentification LDAP ou l'authentification Kerberos. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel appartient l'utilisateur du référentiel PowerCenter. Le nom du domaine de sécurité est sensible à la casse. Si vous ne spécifiez pas cette option, la commande définit le domaine de sécurité de l'utilisateur du référentiel sur le domaine de sécurité que vous spécifiez dans l'option -sdn.
-RepositoryUser -ru	repository_user	Obligatoire. Nom de l'utilisateur du référentiel PowerCenter.
-RepositoryPassword -rp	repository_password	Obligatoire. Mot de passe de l'utilisateur du référentiel PowerCenter. Mot de passe de l'utilisateur. Vous pouvez définir un mot de passe avec l'option -rp ou la variable d'environnement INFA_REPOSITORY_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -rp est prioritaire.

AssignLicense

Assigne une licence à un service d'application. Vous devez assigner une licence à un service d'application avant de pouvoir activer ce dernier.

Remarque: Vous ne pouvez pas attribuer une licence à un service si celui-ci est attribué à une autre licence. Pour attribuer une autre licence à un service, supprimez la licence existante à l'aide de la commande RemoveLicense, puis attribuez la nouvelle licence.

La commande infacmd isp AssignLicense utilise la syntaxe suivante :

```
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 ...
```

Le tableau suivant décrit les options et arguments d'infacmd isp AssignLicense :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-LicenseName -ln	license_name	Obligatoire. Nom de la licence que vous souhaitez attribuer à un service.
-ServiceNames -sn	service_name1 service_name2 ...	Obligatoire. Noms des services auxquels vous souhaitez attribuer une licence. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets. Redémarrez le service pour appliquer les modifications.

AssignRoleToGroup

Assigne un rôle à un groupe pour un domaine ou un service d'application.

La commande infacmd isp AssignRoleToGroup utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp AssignRoleToGroup :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-GroupName -gn	group_name	Obligatoire. Nom du groupe auquel vous attribuez le rôle. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-GroupSecurityDomain -gsf	group_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité du groupe auquel vous attribuez le rôle. La valeur par défaut est Natif.
-RoleName -rn	role_name	Obligatoire. Nom du rôle que vous souhaitez attribuer au groupe.
-ServiceName -sn	service_name	Obligatoire. Nom de service du domaine ou de l'application auquel vous souhaitez attribuer le rôle. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.

AssignRoleToUser

Assigne un rôle à un utilisateur pour un domaine ou un service d'application.

La commande infacmd isp AssignRoleToUser utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp AssignRoleToUser :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ExistingUserName -eu	existing_user_Name	Obligatoire. Compte utilisateur auquel vous attribuez le rôle. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité de l'utilisateur auquel vous attribuez le rôle. La valeur par défaut est Natif.
-RoleName -rn	role_name	Obligatoire. Nom du rôle que vous souhaitez attribuer à l'utilisateur.
-ServiceName -sn	service_name	Obligatoire. Nom de service du domaine ou de l'application auquel vous souhaitez attribuer le rôle. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.

AssignRSToWSHubService

Associe un référentiel PowerCenter à un Hub de services Web dans le domaine.

La commande infacmd isp AssignRSToWSHubService utilise la syntaxe suivante :

```
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
```


Le tableau suivant décrit les options et arguments d'infacmd isp AssignRSToWSHubService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-ServiceName -sn	service_name	Obligatoire. Nom du hub de services Web auquel vous souhaitez associer un référentiel.
-NodeName -nn	node_name	Obligatoire. Nom du nœud sur lequel vous souhaitez que le processus hub de services Web s'exécute. Si l'environnement PowerCenter est configuré pour une haute disponibilité, il s'agit du nom du nœud principal.
-RepositoryService -rs	repository_service_name	Obligatoire. Nom du service de référentiel PowerCenter dont dépend le hub de services Web. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-RepositoryUser -ru	user	Obligatoire. Nom d'utilisateur utilisé pour la connexion au référentiel. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-RepositoryPassword -rp	mot de passe	Obligatoire. Mot de passe de l'utilisateur. Mot de passe de l'utilisateur. Vous pouvez définir un mot de passe avec l'option -rp ou la variable d'environnement INFA_REPOSITORY_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -rp est prioritaire.

AssignUserPermission

Assigne une autorisation d'utilisateur sur un objet.

Les autorisations permettent à un utilisateur d'accéder à des objets dans un domaine. Les objets incluent le domaine, les dossiers, les nœuds, les grilles, les licences et les services d'applications. Par exemple, si vous assignez une autorisation d'utilisateur à un dossier, l'utilisateur hérite de l'autorisation sur tous les objets dans le dossier.

La commande infacmd isp AssignUserPermission utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'*infacmd isp AssignUserPermission* :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT.
-ExistingUserName -eu	existing_user_name	Obligatoire. Nom de l'utilisateur auquel vous souhaitez attribuer une autorisation sur un objet.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité de l'utilisateur auquel vous souhaitez attribuer une autorisation. La valeur par défaut est Natif.
-ObjectName -on	object_name	Obligatoire. Nom de l'objet auquel vous souhaitez affecter l'autorisation d'accès utilisateur.
-ObjectType -ot	object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE	Obligatoire. Type d'objet. Entrez l'une des valeurs suivantes : <ul style="list-style-type: none"> - Service - Licence - Nœud - Grille - Dossier - OSProfile

ConvertLogFile

Convertit les fichiers journaux binaires en fichiers texte, fichiers XML ou encore en texte lisible à l'écran.

La commande infacmd isp ConvertLogFile utilise la syntaxe suivante :

```

ConvertLogFile
<-InputFile|-in> input_file_name
[<-Format|-fm> format_TEXT_XML]
[<-OutputFile|-lo> output_file_name]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ConvertLogFile :

Option	Argument	Description
-InputFile -in	input_file_name	Obligatoire. Nom et chemin d'accès du fichier journal que vous voulez convertir. Par défaut, le gestionnaire de service écrit les fichiers journaux dans le répertoire server\infa_shared\log sur le nœud maître de passerelle.
-Format -fm	format	Facultatif. Format de fichier de sortie. Les types valides comprennent : <ul style="list-style-type: none">- Text- XML Si vous ne spécifiez pas un format, infacmd utilise le format de texte avec des lignes limitées à 80 caractères.
-OutputFile -lo	output_file_name	Facultatif. Le nom et le chemin du fichier pour le fichier de sortie. Si vous ne spécifiez pas un nom de fichier de sortie, infacmd affiche les événements du journal sur l'écran.

convertUserActivityLogFile

Convertit un fichier journal binaire d'activité utilisateur récupéré avec la commande getUserActivityLog au format texte ou XML.

La commande infacmd isp convertUserActivityLogFile utilise la syntaxe suivante :

```
convertUserActivityLogFile  
  
<-InputFile|-in> input_file_name  
  
[<-Format|-fm> format_TEXT_XML]  
  
[<-OutputFile|-lo> output_file_name]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd isp convertUserActivityLogFile :

Option	Argument	Description
-InputFile -in	input_file_name	Obligatoire. Nom du fichier journal à convertir.
-Format -fm	format_TEXT_XML	Facultatif. Format de fichier de sortie. Les formats valides sont les suivants : <ul style="list-style-type: none">- Texte- XML La valeur par défaut est le format texte.
-OutputFile -lo	output_file_name	Facultatif. Nom du fichier de sortie. Si vous ne spécifiez pas de nom de fichier de sortie, la commande affiche le journal sur la ligne de commande.

CreateConnection

Définit une connexion et les options de connexion.

Pour répertorier les options de connexion pour une connexion existante, exécutez infacmd isp ListConnectionOptions.

La commande infacmd isp CreateConnection utilise la syntaxe suivante :

```
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)
```

Le tableau suivant décrit les options et les arguments d'infacmd isp CreateConnection :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConnectionName -cn	connection_name	Nom de la connexion. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Le nom ne peut pas dépasser 128 caractères, contenir des espaces, ou contenir les caractères spéciaux suivants : ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
- ConnectionId -cid	connection_id	Chaîne utilisée par le service d'intégration de données pour identifier la connexion. L'ID n'est pas sensible à la casse. Il peut contenir jusqu'à 255 caractères et doit être unique dans le domaine. Vous ne pouvez pas modifier cette propriété après avoir créé la connexion. La valeur par défaut est le nom de la connexion.

Option	Argument	Description
-ConnectionType -ct	connection_type	<p>Requis. Type de connexion. Utilisez l'un des types de connexion suivants :</p> <ul style="list-style-type: none"> - ADABAS - ADLSGEN1 (Microsoft Azure Data Lake Storage Gen1) - ADLSGEN2 (Microsoft Azure Data Lake Storage Gen2) - AMAZONKINESIS - AMAZONREDSHIFT - AMAZONS3 - AZUREBLOB (Microsoft Azure Blob Storage) - BIGQUERY (Google BigQuery) - BLOCKCHAIN - CASSANDRA - ConfluentKafka - DATABRICKS - DATASIFT - DB2 - DB2I - DB2Z - FACEBOOK - GreenplumPT - GOOGLLEANALYTICS - GOOGLESTORAGEV2 - HADOOP - HBASE - HDFS - HIVE - IBMDB2 - IMS - JDBC - JDBC V2 - JDEDWARDS ENTERPRISE ONE - KAFKA - LDAP - LINKEDIN - MAPR-DB - Microsoft Azure SQL Data Warehouse - MSDYNAMICS - NETEZZA - ODATA - ODBC - ORACLE - SALESFORCE - SFMC (Salesforce Marketing Cloud) - SAPAPPLICATIONS - SEQ - SFDC - SNOWFLAKE - SPANNERGOOGLE (Google Cloud Spanner) - SQLSERVER - TABLEAU - TABLEAU V3 - TERADATA PARALLEL TRANSPORTER - TWITTER - TWITTERSTREAMING - VSAM - WEBCONTENT - KAPOWKATALYST <p>Vous pouvez également utiliser la commande <code>infacmd isp ListConnections</code> pour afficher les types de connexion.</p>

Option	Argument	Description
ConnectionUserName -cun	connection_us er_name	Requis. Nom d'utilisateur de la base de données.

Option	Argument	Description
-ConnectionPassword -cpd	connection_password	<p>Requis. Mot de passe pour le nom d'utilisateur de la base de données. Vous pouvez définir un mot de passe avec l'option -cpd ou la variable d'environnement INFA_DEFAULT_CONNECTION_PASSWORD. Si vous définissez un mot de passe avec les deux options, le mot de passe défini avec l'option -cpd est prioritaire.</p> <p>Si vous créez une connexion ADABAS, DB2I, DB2Z, IMS, SEQ ou VSAM, vous pouvez entrer une phrase secrète PowerExchange valide au lieu d'un mot de passe. Les phrases secrètes permettant d'accéder aux bases de données et aux ensembles de données sur z/OS peuvent comporter de 9 à 128 caractères. Les phrases secrètes permettant d'accéder à DB2 for i5/OS peuvent comporter jusqu'à 31 caractères. Les phrases secrètes peuvent contenir les caractères suivants :</p> <ul style="list-style-type: none"> - Lettres majuscules et minuscules - Numéros de 0 à 9 - Espaces - les caractères spéciaux suivants : ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Remarque: le premier caractère est une apostrophe.</p> <p>Les phrases secrètes ne peuvent pas inclure de guillemets simples ('), de guillemets doubles (") ou de symboles de devise.</p> <p>Si une phrase secrète contient des espaces, vous devez la placer entre guillemets doubles ("), par exemple, "Ceci est un exemple de phrase secrète". Si une phrase secrète contient des caractères spéciaux, vous devez l'encadrer par trois guillemets doubles ("""), par exemple, """"Cette phrase secrète contient des caractères spéciaux ! % & *. """".</p> <p>Si une phrase secrète contient uniquement des caractères alphanumériques sans espaces, vous pouvez l'entrer sans délimiteurs.</p> <p>Remarque: Sur z/OS, une phrase secrète RACF valide peut comporter jusqu'à 100 caractères. PowerExchange tronque les phrases de passe de plus de 100 caractères lorsqu'elles sont transmises à RACF pour la validation.</p> <p>Pour utiliser les phrases secrètes, vérifiez que le service d'écoute PowerExchange est exécuté avec une valeur supérieure ou égale à (1, N) pour le paramètre de sécurité SECURITY dans le membre DBMOVER. Pour plus d'informations, voir la section du <i>Manuel de référence PowerExchange</i> relative à l'instruction SECURITY.</p> <p>Pour utiliser des phrases secrètes pour les connexions IMS, vérifiez que les conditions supplémentaires suivantes sont respectées :</p> <ul style="list-style-type: none"> - Vous devez configurer l'accès ODBA à IMS comme décrit dans le <i>Guide de l'utilisateur Navigateur PowerExchange</i>. - Vous devez utiliser les cartes de données IMS que IMS ODBA spécifie comme la méthode d'accès. N'utilisez pas les cartes de données qui indiquent la méthode d'accès DL/1 BATCH car cette méthode d'accès nécessite l'utilisation des tâches netport, qui ne prennent pas en charge des phrases de passe. - La base de données IMS doit être en ligne dans la région de contrôle IMS pour utiliser l'accès ODBA à IMS.

Option	Argument	Description
-VendorId -vid	vendor_id	Facultatif. ID du partenaire externe qui construit l'adaptateur.
-Options -o	options	Requis. Entrez les paires nom-valeur séparées par des espaces. Les options de connexion sont différentes pour chaque type de connexion. Utilisez un guillemet simple pour échapper tout signe égal ou espace dans la valeur.

Options de connexion ADABAS

Utilisez les options de connexion pour définir une connexion ADABAS.

Entrez les options de connexion au format suivant :

- Séparez les options multiples par un espace.
- Placez les paramètres qui contiennent un signe égal (=) entre guillemets simples.

```
... -o option_name=value option_name=value ...
```

Le tableau suivant décrit les options de connexion Adabas :

Option	Description
CodePage	Requis. Code devant être lu dans la base de données ou écrit dans celle-ci. Utilisez le nom de la page du code ISO, par exemple ISO-8859-6. Le nom de la page du code n'est pas sensible à la casse.
ArraySize	Facultatif. Détermine le nombre d'enregistrements dans la matrice de stockage pour les threads lorsque la valeur des threads de travail est supérieure à 0. Les valeurs valides sont comprises entre 1 et 5 000. La valeur par défaut est 25.
Compression	Facultatif. Comprime les données pour réduire le volume de données que les applications Informatica écrivent sur le réseau. True ou false. La valeur par défaut est False.
EncryptionLevel	Facultatif. Niveau de chiffrement. Si vous spécifiez AES pour l'option EncryptionType, spécifiez l'une des valeurs suivantes pour indiquer le niveau de chiffrement AES : <ul style="list-style-type: none"> - 1. Utilisez une clé de chiffrement 128 bits. - 2. Utilisez une clé de chiffrement 192 bits. - 3. Utilisez une clé de chiffrement 256 bits. La valeur par défaut est 1. Remarque: Si vous sélectionnez Aucun pour le type de chiffrement, le service d'intégration de données ignore la valeur de niveau de chiffrement.
EncryptionType	Facultatif. Vérifie s'il faut utiliser le chiffrement. Spécifiez l'une des valeurs suivantes : <ul style="list-style-type: none"> - Aucun - AES La valeur par défaut est Aucun.
InterpretAsRows	Facultatif. Si la valeur est « Vrai », la taille de stimulation représente un nombre de lignes. Si la valeur est False, la taille de stimulation représente des kilooctets. La valeur par défaut est False.

Option	Description
Emplacement	Emplacement du nœud Écouteur PowerExchange qui peut se connecter à la base de données. L'emplacement est défini dans le premier paramètre de l'instruction NODE dans le fichier de configuration dbmover.cfg de PowerExchange.
OffLoadProcessing	Facultatif. Déplace le traitement des données en bloc depuis la machine source vers la machine du service d'intégration de données. Entrez l'une des valeurs suivantes : <ul style="list-style-type: none"> - Auto. Le service d'intégration de données détermine si vous souhaitez utiliser le traitement de déchargement. - Oui. Utiliser le traitement de déchargement. - Non. Ne pas utiliser le traitement de déchargement. La valeur par défaut est Auto.
PacingSize	Facultatif. Ralentit le taux de transfert de données pour réduire les goulets d'étranglement. Plus la valeur est basse, plus les performances de la session sont élevées. La valeur minimale est 0. Entrez 0 pour des performances optimales. La valeur par défaut est 0.
WorkerThread	Facultatif. Nombre de threads que le service d'intégration de données utilise pour traiter les données en bloc lorsque le traitement du déchargement est activé. Pour des performances optimales, cette valeur ne doit pas dépasser le nombre de processeurs disponibles sur la machine du service d'intégration de données. Les valeurs valides vont de 1 à 64. La valeur par défaut est 0, ce qui désactive le multithreading.
WriteMode	Entrez l'un des modes d'écriture suivants : <ul style="list-style-type: none"> - CONFIRMWRITEON. Envoie des données à l'Écouteur PowerExchange et attend la réponse de réussite/échec avant d'envoyer davantage de données. - CONFIRMWRITEOFF. Envoie des données à l'Écouteur PowerExchange sans attendre la réponse de réussite/échec. Utilisez cette option lorsque la table cible peut être rechargée si une erreur se produit. - ASYNCHRONOUSWITHFAULTT. Envoie des données à l'Écouteur PowerExchange de manière asynchrone avec la possibilité de détecter les erreurs. La valeur par défaut est CONFIRMWRITEON.
EnableConnectionPool	Facultatif. Active le pooling de connexions. Lorsque vous activez le pooling de connexions, celui-ci conserve les instances de connexion inactives en mémoire. Lorsque vous désactivez le pooling de connexions, le service d'intégration de données arrête toute l'activité du pooling. True ou false. La valeur par défaut est False.
ConnectionPoolSize	Facultatif. Nombre maximal d'instances de connexion inactives que le service d'intégration de données gère pour une connexion de base de données. Définissez cette valeur à une valeur supérieure au nombre minimal d'instances de connexion inactives. La valeur par défaut est 15.
ConnectionPoolMaxIdleTime	Facultatif. Nombre de secondes pendant lesquelles une connexion qui dépasse le nombre minimal d'instances de connexion peut rester inactive avant que le pool de connexions ne l'abandonne. Le pool de connexions ignore la durée d'inactivité lorsque celle-ci ne dépasse pas le nombre minimal d'instances de connexion inactives. La valeur par défaut est 120.
ConnectionPoolMinConnections	Facultatif. Nombre minimal d'instances de connexion inactives que le pool maintient pour une connexion de base de données. Définissez cette valeur comme étant égale ou inférieure à la taille du pool de connexions inactives. La valeur par défaut est 0.

Options de connexion Amazon Kinesis

Utilisez les options de connexion pour définir une connexion Amazon Kinesis.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour créer, par exemple, une connexion Amazon Kinesis à Kinesis Streams sous UNIX à l'aide du rôle IAM inter-compte, exécutez la commande suivante :

```
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'"
```

Pour créer une connexion Amazon Kinesis à Kinesis Firehose sous UNIX à l'aide du profil d'informations d'identification AWS, exécutez la commande suivante :

```
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'"
```

Pour entrer plusieurs options, séparez-les par des espaces. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Amazon Kinesis pour la commande `infacmd` `isp` `CreateConnection` :

Propriété	Description
AWS_ACCESS_KEY_ID	ID de clé d'accès du compte d'utilisateur Amazon AWS.
AWS_SECRET_ACCESS_KEY	Clé d'accès secrète de votre compte d'utilisateur Amazon AWS.
ConnectionTimeOut	Délai d'attente en millisecondes du service d'intégration avant d'établir une connexion au flux Kinesis ou à Kinesis Firehose, après quoi il expire.
Region	Région dans laquelle le point de terminaison de votre service est disponible. Vous pouvez sélectionner l'une des valeurs suivantes : <ul style="list-style-type: none">- us-east-2. Indique la région Est des États-Unis (Ohio).- us-east-1. Indique la région Est des États-Unis (Virginie du Nord).- us-west-1. Indique la région Ouest des États-Unis (Californie du Nord).- us-west-2. Indique la région Ouest des États-Unis (Oregon).- ap-northeast-1. Indique la région Asie-Pacifique (Tokyo).- ap-northeast-2. Indique la région Asie-Pacifique (Séoul).- ap-northeast-3. Indique la région Asie-Pacifique (Osaka-Local).- ap-south-1. Indique la région Asie-Pacifique (Bombay).- ap-southeast-1. Indique la région Asie-Pacifique (Singapour).- ap-southeast-2. Indique la région Asie-Pacifique (Sydney).- ca-central-1. Indique la région Canada (Central).- cn-north-1. Indique la région Chine (Pékin).- cn-northwest-1. Indique la région Chine (Ningxia).- eu-central-1. Indique la région Union européenne (Francfort).- eu-west-1. Indique la région Union européenne (Irlande).- eu-west-2. Indique la région Union européenne (Londres).- eu-west-3. Indique la région Union européenne (Paris).- sa-east-1. Indique la région Amérique du Sud (São Paulo).

Propriété	Description
ServiceType	Type de service Kinesis auquel la connexion est associée. Sélectionnez l'un des types de services suivants : - Kinesis Firehose. Sélectionnez ce service pour écrire dans le flux de diffusion Kinesis Firehose. - Kinesis Streams. Sélectionnez ce service pour lire depuis Kinesis Streams.
ProfileName	Obligatoire si vous utilisez le type d'authentification du profil d'informations d'identification AWS. Profil d'informations d'identification AWS défini dans le fichier d'informations d'identification. Un mappage accède aux informations d'identification AWS via le nom du profil lors de l'exécution. Si vous n'indiquez pas un nom de profil d'informations d'identification AWS, le mappage utilise l'ID de clé d'accès et la clé d'accès secrète que vous spécifiez lors de la création de la connexion.
RoleArn	Obligatoire si vous utilisez le type d'authentification par rôle IAM inter-compte. Nom de ressource Amazon spécifiant le rôle d'un utilisateur IAM.
ExternalID	Obligatoire si vous utilisez le type d'authentification par rôle IAM inter-compte et que l'ID externe est défini par le compte AWS. L'ID externe d'un rôle IAM est une restriction supplémentaire que vous pouvez utiliser dans une stratégie d'approbation de rôle IAM pour désigner celui qui remplit le rôle IAM.
AuthenticationType	Type d'authentification. Sélectionnez l'une des valeurs suivantes : - Profil des informations d'identification AWS - Rôle IAM inter-compte La valeur par défaut est Profil d'informations d'identification AWS.

Options de connexion d'Amazon Redshift

Utilisez les options de connexion pour définir une connexion Amazon Redshift.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par des espaces. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Amazon Redshift obligatoires pour les commandes `infacmd isp CreateConnection` et `UpdateConnection` :

Propriété	Description
Nom d'utilisateur	Nom d'utilisateur du compte Amazon Redshift.
Mot de passe	Mot de passe du compte Amazon Redshift.
ID de clé d'accès	ID de clé d'accès aux compartiments Amazon S3. Remarque: Requis si vous n'utilisez pas l'authentification AWS Identity et Access Management (IAM).

Propriété	Description
Clé d'accès secrète	ID de clé d'accès secrète aux compartiments Amazon S3. Remarque: Requis si vous n'utilisez pas l'authentification AWS Identity et Access Management (IAM).
Clé symétrique principale	Facultatif. Fournissez une clé de chiffrement AES de 256 bits au format Base64 lorsque vous activez le chiffrement côté client. Vous pouvez générer une clé à l'aide d'un outil tiers. Si vous spécifiez une valeur, veuillez à spécifier le type de chiffrement en tant que chiffrement côté client dans les propriétés cibles avancées.
URL JDBC	URL de connexion Amazon Redshift.
Région de cluster	Facultatif. Région de cluster AWS dans laquelle réside le compartiment auquel vous souhaitez accéder. Sélectionnez une région de cluster si vous choisissez de fournir une URL JDBC personnalisée qui ne contient pas un nom de région de cluster dans la propriété de connexion URL JDBC . Si vous spécifiez une région de cluster dans les deux propriétés de connexion Région de cluster et URL JDBC , le service d'intégration de données ignore la région de cluster que vous spécifiez dans la propriété de connexion URL JDBC . Pour utiliser le nom de région de cluster que vous spécifiez dans la propriété de connexion URL JDBC , sélectionnez Aucun comme région de cluster dans cette propriété. Sélectionnez l'une des régions de cluster suivantes : Sélectionnez l'une des régions suivantes : <ul style="list-style-type: none"> - Asie-Pacifique (Mumbai) - Asie-Pacifique (Séoul) - Asie-Pacifique (Singapour) - Asie-Pacifique (Sydney) - Asie-Pacifique (Tokyo) - AWS GovCloud (États-Unis) - Canada (Centre) - Chine (Beijing) - Chine (Ningxia) - Union Européenne (Irlande) - Union Européenne (Francfort) - Union Européenne (Londres) - Union Européenne (Paris) - Amérique du Sud (Sao Paulo) - Est des États-Unis (Ohio) - Est des États-Unis (Virginie du Nord) - Ouest des États-Unis (Californie du Nord) - Ouest des États-Unis (Oregon) La valeur par défaut est Aucun . Vous pouvez uniquement lire ou écrire les données dans les régions de cluster prises en charge par le SDK AWS utilisé par PowerExchange for Amazon Redshift.
ID de clé principale client	Facultatif. Spécifiez l'ID de clé principale client généré par AWS Key Management Service (AWS KMS) ou par le nom Amazon Resource Name (ARN) de votre clé personnalisée pour l'accès inter-comptes. Vous devez générer la clé principale client correspondant à la région où se trouvent les compartiments Amazon S3. Vous pouvez indiquer l'une des valeurs suivantes : Clé principale client générée par le client Active le chiffrement côté client ou côté serveur. Clé principale client par défaut Active le chiffrement côté client ou côté serveur. Seul l'utilisateur administrateur du compte peut utiliser l'ID de clé principale client par défaut pour activer le chiffrement côté client.

Options de connexion Amazon S3

Utilisez les options de connexion pour définir une connexion Amazon S3.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par des espaces. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Amazon S3 obligatoires pour les commandes `infacmd isp CreateConnection` et `UpdateConnection` :

Propriété	Description
Nom	Le nom de la connexion. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Vous pouvez modifier cette propriété après avoir créé la connexion. Le nom ne peut pas dépasser 128 caractères, ni contenir des espaces ni les caractères spéciaux suivants : ~ ` ! \$ % ^ & * () - + = { }] \ ; " ' < , > . ? /
ID	Chaîne utilisée par le service d'intégration de données pour identifier la connexion. L'ID n'est pas sensible à la casse. Il peut contenir jusqu'à 255 caractères et doit être unique dans le domaine. Vous ne pouvez pas modifier cette propriété après avoir créé la connexion. La valeur par défaut est le nom de la connexion.
Description	Facultatif. La description de la connexion. La description ne peut pas dépasser 4 000 caractères.
Emplacement	Domaine dans lequel vous voulez créer la connexion.
Type	Le type de connexion Amazon S3.
Clé d'accès	Clé d'accès au compartiment Amazon S3. Fournissez la valeur de clé d'accès en fonction des méthodes d'authentification suivantes : <ul style="list-style-type: none">- Authentification de base : fournissez la valeur de clé d'accès réelle.- Authentification IAM : ne fournissez pas la valeur de clé d'accès.- Informations d'identification de sécurité temporaires via le rôle assumé : fournissez la clé d'accès d'un utilisateur IAM sans autorisation pour accéder au compartiment Amazon S3.
Clé secrète	Clé d'accès secrète au compartiment Amazon S3. La clé secrète est associée à la clé d'accès et identifie de façon unique le compte. Fournissez la valeur de clé d'accès en fonction des méthodes d'authentification suivantes : <ul style="list-style-type: none">- Authentification de base : fournissez la valeur de clé d'accès secrète réelle.- Authentification IAM : ne fournissez pas la valeur de clé d'accès secrète.- Informations d'identification de sécurité temporaires via le rôle assumé : fournissez la clé d'accès secrète d'un utilisateur IAM sans autorisation pour accéder au compartiment Amazon S3.
ARN de rôle IAM	ARN du rôle IAM pris par l'utilisateur pour utiliser les informations d'identification de sécurité temporaires générées de manière dynamique. Entrez la valeur de cette propriété si vous souhaitez utiliser les informations d'identification de sécurité temporaires pour accéder aux ressources AWS. Si vous souhaitez utiliser les informations d'identification de sécurité temporaires avec l'authentification IAM, ne spécifiez aucune valeur pour les propriétés de connexion Clé d'accès et Clé secrète. Si vous souhaitez utiliser les informations d'identification de sécurité temporaires sans l'authentification IAM, spécifiez une valeur pour les propriétés de connexion Clé d'accès et Clé secrète. Pour plus d'informations sur l'obtention de l'ARN du rôle IAM, consultez la documentation AWS.

Propriété	Description
Chemin du dossier	<p>Le chemin d'accès complet aux objets Amazon S3. Le chemin doit inclure le nom du compartiment et les noms des dossiers.</p> <p>N'utilisez pas de barre oblique à la fin du chemin du dossier. Par exemple, <nom du compartiment>/<nom de mon dossier>.</p>
Clé symétrique principale	<p>Facultatif. Fournissez une clé de chiffrement AES de 256 bits au format Base64 lorsque vous activez le chiffrement côté client. Vous pouvez générer une clé symétrique principale à l'aide d'un outil tiers.</p>
Type de compte S3	<p>Type du compte Amazon S3.</p> <p>Sélectionnez Stockage Amazon S3 ou Stockage compatible S3.</p> <p>Sélectionnez l'option de stockage Amazon S3 pour utiliser les services Amazon S3. Sélectionnez l'option de stockage compatible S3 pour spécifier le point de terminaison d'un fournisseur de stockage tiers tel que Scality RING.</p> <p>Par défaut, le stockage Amazon S3 est sélectionné.</p>
Point de terminaison REST	<p>Point de terminaison de stockage S3.</p> <p>Spécifiez le point de terminaison de stockage S3 au format HTTP/HTTPs lorsque vous sélectionnez l'option de stockage compatible S3. Par exemple, http://s3.isv.scality.com.</p>
Nom de région	<p>Sélectionnez la région AWS dans laquelle réside le compartiment auquel vous souhaitez accéder.</p> <p>Sélectionnez l'une des régions suivantes :</p> <ul style="list-style-type: none"> - Asie-Pacifique (Mumbai) - Asie-Pacifique (Séoul) - Asie-Pacifique (Singapour) - Asie-Pacifique (Sydney) - Asie-Pacifique (Tokyo) - AWS GovCloud (États-Unis) - Canada (Centre) - Chine (Beijing) - Chine (Hong Kong) - Chine (Ningxia) - Union Européenne (Irlande) - Union Européenne (Francfort) - Union Européenne (Londres) - Union Européenne (Paris) - Amérique du Sud (Sao Paulo) - Est des États-Unis (Ohio) - Est des États-Unis (Virginie du Nord) - Ouest des États-Unis (Californie du Nord) - Ouest des États-Unis (Oregon) <p>La valeur par défaut est Est des États-Unis (Virginie du Nord).</p> <p>Non applicable pour le stockage compatible S3.</p>

Propriété	Description
ID de clé principale client	<p>Facultatif. Spécifiez l'ID de clé principale client ou le nom d'alias généré par AWS Key Management Service (AWS KMS) ou par le nom Amazon Resource Name (ARN) de votre clé personnalisée pour l'accès inter-comptes. Vous devez générer la clé principale client pour la région où se trouve le compartiment Amazon S3.</p> <p>Vous pouvez indiquer l'une des valeurs suivantes :</p> <p>Clé principale client générée par le client</p> <p>Active le chiffrement côté client ou côté serveur.</p> <p>Clé principale client par défaut</p> <p>Active le chiffrement côté client ou côté serveur. Seul l'utilisateur administrateur du compte peut utiliser l'ID de clé principale client par défaut pour activer le chiffrement côté client.</p>
IdP SSO fédéré	<p>Fournisseur d'identité compatible SAML 2.0 pour l'authentification unique des utilisateurs fédérés à utiliser avec le compte AWS.</p> <p>PowerExchange for Amazon S3 prend en charge uniquement le fournisseur d'identité ADFS 3.0.</p> <p>Sélectionnez Aucun si vous ne souhaitez pas utiliser l'authentification unique des utilisateurs fédérés.</p>

Propriétés de connexion d'authentification unique des utilisateurs fédérés

Configurez les propriétés suivantes lorsque vous sélectionnez ADFS 3.0 sous **IdP SSO fédéré** :

Propriété	Description
Nom d'utilisateur fédéré	Nom de l'utilisateur fédéré permettant d'accéder au compte AWS via le fournisseur d'identité.
Mot de passe de l'utilisateur fédéré	Mot de passe de l'utilisateur fédéré permettant d'accéder au compte AWS via le fournisseur d'identité.
URL SSO de l'IdP	URL d'authentification unique du fournisseur d'identité pour AWS.
ARN du fournisseur d'identité SAML	ARN du fournisseur d'identité SAML que l'administrateur AWS a créé pour enregistrer le fournisseur d'identité en tant que fournisseur approuvé.
ARN de rôle	ARN du rôle IAM attribué à l'utilisateur fédéré.

Options de connexion de blockchain

Utilisez les options de connexion pour définir une connexion de blockchain.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par des espaces. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion de blockchain pour les commandes `infacmd isp CreateConnection` et `UpdateConnection` :

Propriété	Description
<code>swaggerFilePath</code>	Chemin absolu du fichier Swagger qui contient l'API REST pour communiquer avec la blockchain. Le fichier Swagger doit être un fichier JSON stocké sur la machine exécutant le service d'intégration de données. Si le fichier Swagger est à un format de fichier différent, tel que YAML, convertissez le fichier en format JSON.
<code>authType*</code>	Méthode d'authentification que le moteur d'exécution utilise pour la connexion au serveur REST. Vous pouvez utiliser les types suivants : <code>none</code> , <code>basic</code> , <code>digest</code> ou <code>OAuth</code> .
<code>authUserID*</code>	Nom d'utilisateur pour l'authentification auprès du serveur REST.
<code>authPassword*</code>	Mot de passe de l'utilisateur pour l'authentification auprès du serveur REST.
<code>oAuthConsumerKey*</code>	Requis pour le type d'authentification <code>OAuth</code> . Clé du client associée au serveur REST.
<code>oAuthConsumerSecret*</code>	Requis pour le type d'authentification <code>OAuth</code> . Mot de passe du client pour la connexion au serveur REST.
<code>oAuthToken*</code>	Requis pour le type d'authentification <code>OAuth</code> . Jeton d'accès pour la connexion au serveur REST.
<code>oAuthTokenSecret*</code>	Requis pour le type d'authentification <code>OAuth</code> . Mot de passe associé au jeton <code>OAuth</code> .
<code>proxyType*</code>	Type de proxy. Vous pouvez utiliser un proxy de plate-forme, un proxy personnalisé ou aucun proxy.
<code>proxyDetails*</code>	Configuration du proxy utilisant le format <code><host>:<port></code> .
<code>trustStoreFilePath*</code>	Chemin absolu du fichier <code>truststore</code> contenant le certificat SSL.
<code>trustStorePassword*</code>	Mot de passe du fichier <code>truststore</code> .
<code>keyStoreFilePath*</code>	Chemin absolu du fichier <code>keystore</code> qui contient les clés et les certificats requis pour établir une connexion bidirectionnelle sécurisée avec le serveur REST.
<code>keyStorePassword*</code>	Mot de passe du fichier entrepôt de clés.
<code>advancedProperties</code>	<p>Liste des propriétés avancées pour accéder à un actif de la blockchain. Spécifiez les propriétés avancées à l'aide de paires nom-valeur séparées par des points-virgules.</p> <p>Vous pouvez utiliser les propriétés avancées suivantes :</p> <ul style="list-style-type: none"> - <code>baseUrl</code>. Requis si le fichier Swagger ne contient pas l'URL de base. URL de base utilisée pour accéder aux actifs sur la blockchain. - <code>X-API-KEY</code>. Requis si vous effectuez l'authentification sur le serveur REST à l'aide de la clé d'API. <p>Les propriétés avancées que vous configurez dans la connexion remplacent les valeurs des propriétés avancées correspondantes dans l'objet de données de blockchain. Par exemple, si la connexion et l'objet de données spécifient tous deux une URL de base, la valeur dans la connexion remplace la valeur dans l'objet de données.</p>

Propriété	Description
cookies	Requis en fonction de la méthode d'implémentation de l'API REST. Liste des propriétés de cookie pour spécifier les informations de cookie transmises au serveur REST. Spécifiez les propriétés à l'aide de paires nom-valeur séparées par des points-virgules. Les propriétés de cookie que vous configurez dans la connexion remplacent les valeurs des propriétés de cookie correspondantes dans l'objet de données de blockchain.
<p>* La propriété est ignorée. Pour utiliser la fonctionnalité, configurez la propriété en tant que propriété avancée et fournissez une paire nom-valeur basée sur le nom de la propriété dans le fichier Swagger.</p> <p>Par exemple, configurez la paire nom-valeur suivante pour utiliser une autorisation de base :</p> <pre>Authorization=Basic <credentials></pre>	

Options de connexion Cassandra

Utilisez les options de connexion pour définir la connexion Cassandra.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Par exemple :

```
./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;
```

Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Cassandra pour les commandes infacmd isp CreateConnection et UpdateConnection :

Propriété	Description
HostName	Nom d'hôte ou adresse IP du serveur Cassandra.
Port	Numéro de port du serveur Cassandra. La valeur par défaut est 9042.
User Name -cun	Nom d'utilisateur pour accéder au serveur Cassandra.
Password -cpd	Mot de passe correspondant au nom d'utilisateur pour accéder au serveur Cassandra.
DefaultKeyspace	Nom de l'espace de clés Cassandra à utiliser par défaut.

Propriété	Description
SQLIDENTIFIERCHARACTER	<p>Type de caractère que la base de données utilise pour encadrer des identificateurs délimités dans les requêtes SQL ou CQL. Les caractères disponibles dépendent du type de la base de données.</p> <p>Spécifiez Aucun si la base de données utilise des identificateurs classiques. Lorsque le service d'intégration de données génère des requêtes SQL ou CQL, il ne place pas de caractères de délimitation autour des identificateurs.</p> <p>Spécifiez un caractère si la base de données utilise des identificateurs délimités. Lorsque le service d'intégration de données génère des requêtes SQL ou CQL, le service encadre les identificateurs délimités de ce caractère.</p>
SSLMODE	<p>Ne s'applique pas à PowerExchange for Cassandra JDBC.</p> <p>Entrez disabled.</p>
AdditionalConnectionProperties	<p>Entrez au moins un paramètre de connexion JDBC au format suivant :</p> <p><param1>=<value>;<param2>=<value>;<param3>=<value></p> <p>PowerExchange for Cassandra JDBC prend en charge les paramètres de connexion JDBC suivants :</p> <ul style="list-style-type: none"> - BinaryColumnLength - DecimalColumnScale - EnableCaseSensitive - EnableNullInsert - EnablePaging - RowsPerPage - StringColumnLength - VTableSeparator

Options de connexion Confluent Kafka

Utilisez les options de connexion pour définir une connexion Confluent Kafka.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Par exemple, pour créer une connexion Confluent Kafka sous UNIX, exécutez la commande suivante :

```
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>' kafkabrokerVersion='<version>'
schemaregistryurl='<schema registry URL>'"
```

Options de connexion Databricks

Utilisez les options de connexion pour définir une connexion Databricks.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Databricks pour les commandes `infacmd isp CreateConnection` et `UpdateConnection` :

Option	Description
<code>connectionId</code>	Chaîne utilisée par le service d'intégration de données pour identifier la connexion. L'ID n'est pas sensible à la casse. Il peut contenir jusqu'à 255 caractères et doit être unique dans le domaine. Vous ne pouvez pas modifier cette propriété après avoir créé la connexion. La valeur par défaut est le nom de la connexion.
<code>connectionType</code>	Requis. Le type de connexion est Databricks.
<code>nom</code>	Le nom de la connexion. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Vous pouvez modifier cette propriété après avoir créé la connexion. Le nom ne peut pas dépasser 128 caractères, ni contenir des espaces ni les caractères spéciaux suivants : <code>~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /</code>
<code>databricksExecutionParameterList</code>	Propriétés avancées spécifiques au moteur Databricks Spark. Pour entrer plusieurs propriétés, séparez chaque paire nom-valeur avec le texte suivant : <code>&:.</code> N'utilisez les propriétés avancées d'Informatica uniquement à la demande du support client international Informatica.
<code>clusterConfigId</code>	Nom de la configuration de cluster associé à l'environnement Databricks. Obligatoire si vous ne configurez pas la configuration du provisionnement de nuage.
<code>provisionConnectionId</code>	Nom de la configuration de provisionnement de nuage associé à une plate-forme de nuage, telle que Microsoft Azure. Obligatoire si vous ne configurez pas la configuration de cluster.
<code>stagingDirectory</code>	Répertoire dans lequel le moteur Databricks Spark stocke temporairement les fichiers d'exécution. Si vous spécifiez un répertoire inexistant, le service d'intégration de données le crée lors de l'exécution. Si vous n'indiquez aucun chemin de répertoire, les fichiers intermédiaires d'exécution sont enregistrés dans <code><cluster staging directory>/DATABRICKS</code> .

Options de connexion DataSift

Utilisez les options de connexion pour définir une connexion DataSift.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion DataSift pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
userName	Nom d'utilisateur DataSift pour le compte d'utilisateur DataSift.
apiKey	Clé API. La clé API de Developer est affichée dans le tableau de bord ou sur la page Paramètres du compte DataSift.

Options de connexion DB2 pour i5/OS

Utilisez les options de connexion DB2I pour définir la connexion DB2 pour i5/OS.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion DB2 pour i5/OS pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
DatabaseName	Nom d'instance de la base de données.
EnvironmentSQL	Facultatif. Commandes SQL permettant de définir l'environnement de base de données lorsque vous vous connectez à la base de données. Le service d'intégration de données exécute le SQL de l'environnement de connexion à chaque connexion à la base de données. Remarque: Placez les caractères spéciaux entre guillemets doubles.
CodePage	Requis. Page de code utilisée pour la lecture depuis une base de données source ou pour l'écriture dans une base de données ou un fichier cible.
ArraySize	Facultatif. Détermine le nombre d'enregistrements dans la matrice de stockage pour les threads lorsque la valeur des threads de travail est supérieure à 0. Les valeurs valides sont comprises entre 1 et 5 000. La valeur par défaut est 25.
Compression	Facultatif. Compresse les données pour réduire le volume de données écrit sur le réseau. La valeur par défaut est False.
EncryptionLevel	Facultatif. Niveau de chiffrement. Si vous spécifiez AES pour l'option EncryptionType, spécifiez l'une des valeurs suivantes pour indiquer le niveau de chiffrement AES : <ul style="list-style-type: none"> - 1. Utilisez une clé de chiffrement 128 bits. - 2. Utilisez une clé de chiffrement 192 bits. - 3. Utilisez une clé de chiffrement 256 bits. La valeur par défaut est 1. Remarque: Si vous sélectionnez Aucun pour le type de chiffrement, le service d'intégration de données ignore la valeur de niveau de chiffrement.
EncryptionType	Facultatif. Vérifie s'il faut utiliser le chiffrement. Spécifiez l'une des valeurs suivantes : <ul style="list-style-type: none"> - Aucun - AES La valeur par défaut est Aucun.

Option	Description
InterpretAsRows	Facultatif. Représente la taille de stimulation sous la forme d'un nombre de lignes. Si la valeur est False, la taille de stimulation représente des kilooctets. La valeur par défaut est False.
Emplacement	Emplacement du nœud Écouteur PowerExchange qui peut se connecter à la base de données. L'emplacement est défini dans le premier paramètre de l'instruction NODE dans le fichier de configuration dbmover.cfg de PowerExchange.
PacingSize	Facultatif. Quantité de données que le système source peut transmettre à l'Écouteur PowerExchange. Configure la taille de stimulation si une application externe, une base de données ou le nœud service d'intégration de données est un goulet d'étranglement. Plus la valeur est basse, plus les performances sont bonnes. La valeur minimale est 0. Entrez 0 pour obtenir des performances maximales. La valeur par défaut est 0.
RejectFile	Facultatif. Entrez le nom et le chemin d'accès du fichier de rejet. Les fichiers de rejet contiennent les lignes qui n'ont pas été écrites dans la base de données.
WriteMode	Entrez l'un des modes d'écriture suivants : <ul style="list-style-type: none"> - CONFIRMWRITEON. Envoie des données à l'Écouteur PowerExchange et attend la réponse de réussite/échec avant d'envoyer davantage de données. - CONFIRMWRITEOFF. Envoie des données à l'Écouteur PowerExchange sans attendre la réponse de réussite/échec. Utilisez cette option lorsque la table cible peut être rechargée si une erreur se produit. - ASYNCHRONOUSWITHFAULTT. Envoie des données à l'Écouteur PowerExchange de manière asynchrone avec la possibilité de détecter les erreurs. La valeur par défaut est CONFIRMWRITEON.
DatabaseFileOverrides	Spécifie l'écrasement du fichier de base de données i5/OS. Le format est le suivant : <code>from_file/to_library/to_file/to_member</code> Où : <ul style="list-style-type: none"> - <i>from_file</i> est le fichier à écraser - <i>to_library</i> est la nouvelle bibliothèque à utiliser - <i>to_file</i> est le fichier dans la nouvelle bibliothèque à utiliser - <i>to_member</i> est facultatif et est le membre dans la nouvelle bibliothèque et le fichier à utiliser La valeur *FIRST est utilisée si rien n'est précisé. Vous pouvez spécifier jusqu'à 8 écrasements de fichiers uniques sur une seule connexion. Un seul remplacement s'applique à une seule source ou une seule cible. Lorsque vous spécifiez plusieurs écrasements de fichiers, placez les chaînes d'écrasement de fichier entre guillemets doubles et ajoutez un espace entre chaque écrasement de fichier. Remarque: Si LibraryList et DatabaseFileOverrides sont spécifiés et qu'une table existe dans les deux, DatabaseFileOverrides est prioritaire.
IsolationLevel	Valide la portée de la transaction. Sélectionnez l'une des valeurs suivantes : <ul style="list-style-type: none"> - Aucun - SC. Stabilité du curseur. - LR. Lecture répétable. - MOD. Modification. - ALL La valeur par défaut est CS.

Option	Description
LibraryList	Liste des bibliothèques que PowerExchange parcourt pour qualifier le nom de la table pour les instructions Select, Insert, Delete ou Update. PowerExchange recherche dans la liste si le nom de la table n'est pas qualifié. Bibliothèques séparées par des virgules. Remarque: Si LibraryList et DatabaseFileOverrides sont spécifiés et qu'une table existe dans les deux, DatabaseFileOverrides est prioritaire.
EnableConnectionPool	Facultatif. Active le traitement parallèle lors du chargement des données dans une table en mode groupé. Utilisé pour Oracle. True ou false. La valeur par défaut est True.
ConnectionPoolSize	Facultatif. Nombre maximal d'instances de connexion inactives que le service d'intégration de données gère pour une connexion de base de données. Définissez cette valeur pour qu'elle soit supérieure au nombre minimal d'instances de connexions inactives.
ConnectionPoolMaxIdleTime	Facultatif. Nombre de secondes pendant lesquelles une connexion qui dépasse le nombre minimal d'instances de connexion peut rester inactive avant que le pool de connexions ne l'abandonne. Le pool de connexions ignore la durée d'inactivité lorsque celle-ci ne dépasse pas le nombre minimal d'instances de connexion inactives.
ConnectionPoolMinConnections	Facultatif. Nombre minimal d'instances de connexion inactives que le pool maintient pour une connexion de base de données. Définissez cette valeur comme étant égale ou inférieure à la taille du pool de connexions inactives. La valeur par défaut est 0.

Options de connexion DB2 for z/OS

Utilisez les options de connexion DB2Z pour définir des connexions IBM DB2 z/OS.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion DB2Z pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
DataAccessConnectionString	Chaîne de connexion utilisée pour accéder aux données de la base de données. <nom de la base de données>
EnvironmentSQL	Facultatif. Commandes SQL permettant de définir l'environnement de base de données lorsque vous vous connectez à la base de données. Le service d'intégration de données exécute le SQL de l'environnement de connexion à chaque connexion à la base de données. Remarque: Placez les caractères spéciaux entre guillemets doubles.
CodePage	Requis. Page de code utilisée pour la lecture depuis une base de données source ou pour l'écriture dans une base de données ou un fichier cible.
ArraySize	Facultatif. Détermine le nombre d'enregistrements dans la matrice de stockage pour les threads lorsque la valeur des threads de travail est supérieure à 0. Les valeurs valides sont comprises entre 1 et 5 000. La valeur par défaut est 25.

Option	Description
Compression	Facultatif. Compresse les données pour réduire le volume de données écrit sur le réseau. La valeur par défaut est False.
CorrelationID	Facultatif. Libellé à appliquer à une tâche ou requête DB2 pour permettre à DB2 for z/OS de prendre en compte les ressources. Entrez jusqu'à 8 octets de caractères alphanumériques.
EncryptionLevel	<p>Facultatif. Niveau de chiffrement. Si vous spécifiez AES pour l'option EncryptionType, spécifiez l'une des valeurs suivantes pour indiquer le niveau de chiffrement AES :</p> <ul style="list-style-type: none"> - 1. Utilisez une clé de chiffrement 128 bits. - 2. Utilisez une clé de chiffrement 192 bits. - 3. Utilisez une clé de chiffrement 256 bits. <p>La valeur par défaut est 1.</p> <p>Remarque: Si vous sélectionnez Aucun pour le type de chiffrement, le service d'intégration de données ignore la valeur de niveau de chiffrement.</p>
EncryptionType	<p>Facultatif. Vérifie s'il faut utiliser le chiffrement. Spécifiez l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> - Aucun - AES <p>La valeur par défaut est Aucun.</p>
InterpretAsRows	Facultatif. Représente la taille de stimulation sous la forme d'un nombre de lignes. Si la valeur est False, la taille de stimulation représente des kilooctets. La valeur par défaut est False.
Emplacement	Emplacement du nœud d'écoute PowerExchange qui peut se connecter à la base de données. Le nœud est défini dans le fichier de configuration dbmover.cfg de PowerExchange.
OffloadProcessing	<p>Facultatif. Déplace le traitement des données en bloc depuis la machine VSAM à la machine du service d'intégration de données.</p> <p>Entrez l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> - Auto. Le service d'intégration de données détermine si vous souhaitez utiliser le traitement de déchargement. - Oui. Utiliser le traitement de déchargement. - Non. Ne pas utiliser le traitement de déchargement. <p>La valeur par défaut est Auto.</p>
PacingSize	<p>Facultatif. Quantité de données que le système source peut transmettre à l'Écouteur PowerExchange. Configure la taille de stimulation si une application externe, une base de données ou le nœud service d'intégration de données est un goulet d'étranglement. Plus la valeur est basse, plus les performances sont bonnes.</p> <p>La valeur minimale est 0. Entrez 0 pour obtenir des performances maximales. La valeur par défaut est 0.</p>
RejectFile	Facultatif. Entrez le nom et le chemin d'accès du fichier de rejet. Les fichiers de rejet contiennent les lignes qui n'ont pas été écrites dans la base de données.
WorkerThread	Facultatif. Nombre de threads que le service d'intégration de données utilise pour traiter les données en bloc lorsque le traitement du déchargement est activé. Pour des performances optimales, cette valeur ne doit pas dépasser le nombre de processeurs disponibles sur la machine du service d'intégration de données. Les valeurs valides vont de 1 à 64. La valeur par défaut est 0, ce qui désactive le multithreading.

Option	Description
WriteMode	Entrez l'un des modes d'écriture suivants : - CONFIRMWRITEON. Envoie des données à l'Écouteur PowerExchange et attend la réponse de réussite/échec avant d'envoyer davantage de données. - CONFIRMWRITEOFF. Envoie des données à l'Écouteur PowerExchange sans attendre la réponse de réussite/échec. Utilisez cette option lorsque la table cible peut être rechargée si une erreur se produit. - ASYNCHRONOUSWITHFAULTT. Envoie des données à l'Écouteur PowerExchange de manière asynchrone avec la possibilité de détecter les erreurs. La valeur par défaut est CONFIRMWRITEON.
EnableConnectionPool	Facultatif. Active le traitement parallèle lors du chargement des données dans une table en mode groupé. Utilisé pour Oracle. True ou false. La valeur par défaut est True.
ConnectionPoolSize	Facultatif. Nombre maximal d'instances de connexion inactives que le service d'intégration de données gère pour une connexion de base de données. Définissez cette valeur pour qu'elle soit supérieure au nombre minimal d'instances de connexions inactives.
ConnectionPoolMaxIdleTime	Facultatif. Nombre de secondes pendant lesquelles une connexion qui dépasse le nombre minimal d'instances de connexion peut rester inactive avant que le pool de connexions ne l'abandonne. Le pool de connexions ignore la durée d'inactivité lorsque celle-ci ne dépasse pas le nombre minimal d'instances de connexion inactives.
ConnectionPoolMinConnections	Facultatif. Nombre minimal d'instances de connexion inactives que le pool maintient pour une connexion de base de données. Définissez cette valeur comme étant égale ou inférieure à la taille du pool de connexions inactives. La valeur par défaut est 0.

Options de connexion Facebook

Utilisez les options de connexion pour définir une connexion Facebook.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Facebook pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
ConsumerKey	L'ID d'application que vous obtenez lorsque vous créez l'application dans Facebook. Facebook utilise la clé pour identifier l'application.
ConsumerSecret	Le secret de l'application que vous obtenez lorsque vous créez l'application dans Facebook. Facebook utilise ce secret pour établir la propriété de la clé du consommateur.
AccessToken	Jeton d'accès que l'utilitaire Oauth renvoie. Facebook utilise ce jeton au lieu des justificatifs d'identité de l'utilisateur pour accéder aux ressources protégées.

Option	Description
AccessSecret	Le secret d'accès n'est pas nécessaire pour une connexion Facebook.
Étendue	Les autorisations pour l'application. Entrez les autorisations que vous avez utilisées pour configurer OAuth.

Options de connexion Greenplum

Utilisez les options de connexion pour définir une connexion Greenplum.

Entrez les options de connexion au format suivant :

... -o option_name=value option_name=value ...

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Greenplum pour les commandes `infacmd isp` `CreateConnection` et `UpdateConnection` :

Option	Description
UserName	Requis. Nom d'utilisateur avec des autorisations d'accès à la base de données Greenplum.
Mot de passe	Requis. Mot de passe de connexion à la base de données Greenplum.
driverName	Requis. Nom du pilote JDBC Greenplum. Par exemple : <code>com.pivotal.jdbc.GreenplumDriver</code> Pour plus d'informations sur le pilote, consultez la documentation Greenplum.
connectionString	Requis. URL de connexion JDBC Greenplum. Par exemple : <code>jdbc:pivotal:greenplum://<nom d'hôte>:<port>;DatabaseName=<nom de la base de données></code> Pour plus d'informations sur l'URL de connexion, consultez la documentation Greenplum.
hostName	Requis. Nom d'hôte ou adresse IP du serveur Greenplum.
portNumber	Facultatif. Numéro de port du serveur Greenplum. Si vous entrez 0, l'utilitaire <code>gpload</code> lit le contenu de la variable d'environnement <code>\$PGPORT</code> . La valeur par défaut est 5432.
databaseName	Requis. Nom de la base de données à laquelle vous souhaitez vous connecter.
enableSSL	Requis. Définissez cette option pour établir une communication sécurisée entre l'utilitaire <code>gpload</code> et le serveur Greenplum sur le SSL.
SSLCertificatePath	Requis si vous activez le protocole SSL. Chemin menant à l'emplacement où sont stockés les certificats SSL pour le serveur Greenplum.

Options de connexion Google Analytics

Utilisez les options de connexion pour définir la connexion Google Analytics.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Par exemple :

```
./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"
```

Le tableau suivant décrit les options de connexion Google Analytics pour les commandes infacmd isp CreateConnection et UpdateConnection :

Propriété	Description
SERVICEACCOUNTID	Obligatoire. Spécifie la valeur client_email présente dans le fichier JSON que vous téléchargez après avoir créé un compte de service.
SERVICEACCOUNTKEY	Obligatoire. Spécifie la valeur private_key présente dans le fichier JSON que vous téléchargez après avoir créé un compte de service.

Options de connexion Google BigQuery

Utilisez les options de connexion pour définir la connexion Google BigQuery.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Par exemple :

```
./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' " ;
```

Le tableau suivant décrit les options de connexion Google BigQuery pour les commandes infacmd isp CreateConnection et UpdateConnection :

Propriété	Description
CLIENTEMAIL	Obligatoire. Spécifie la valeur client_email présente dans le fichier JSON que vous téléchargez après avoir créé un compte dans Google BigQuery.
PRIVATEKEY	Obligatoire. Spécifie la valeur private_key présente dans le fichier JSON que vous téléchargez après avoir créé un compte dans Google BigQuery.

Propriété	Description
Mode de connexion CONNECTORTYPE	<p>Obligatoire. Mode de connexion à utiliser pour lire les données depuis Google BigQuery ou les écrire dans cet outil.</p> <p>Entrez l'un des modes de connexion suivants :</p> <ul style="list-style-type: none"> - Simple. Aplatit chaque champ de la zone Type de données d'enregistrement en tant que champ distinct dans le mappage. - Hybride. Affiche tous les champs de niveau supérieur de la table Google BigQuery, y compris les champs de type Type de données d'enregistrement. PowerExchange for Google BigQuery affiche le champ Type de données d'enregistrement de niveau supérieur sous la forme d'un champ unique du type de données Chaîne dans le mappage. - Complexe. Affiche toutes les colonnes de la table Google BigQuery sous la forme d'un champ unique du type de données Chaîne dans le mappage. <p>La valeur par défaut est Simple.</p>
Chemin du fichier de définition de schéma SCHEMALOCATION	<p>Obligatoire. Spécifie un répertoire sur la machine cliente où PowerExchange for Google BigQuery doit créer un fichier JSON avec l'exemple de schéma de la table Google BigQuery. Le nom du fichier JSON est le même que celui de la table Google BigQuery.</p> <p>Vous pouvez également spécifier un chemin de stockage dans Google Cloud Storage où PowerExchange for Google BigQuery doit créer un fichier JSON avec l'exemple de schéma de la table Google BigQuery. Vous pouvez télécharger le fichier JSON depuis le chemin de stockage spécifié dans Google Cloud Storage vers une machine locale.</p>
PROJECTID	<p>Obligatoire. Spécifie la valeur project_id présente dans le fichier JSON que vous téléchargez après avoir créé un compte dans Google BigQuery.</p> <p>Si vous avez créé plusieurs projets avec le même compte de service, saisissez l'ID du projet qui contient l'ensemble de données auquel vous voulez vous connecter.</p>
STORAGEPATH	<p>Requise pour la lecture ou l'écriture de grands volumes de données.</p> <p>Chemin dans Google Cloud Storage où PowerExchange for Google BigQuery crée un fichier intermédiaire local pour le stockage temporaire des données.</p> <p>Vous pouvez entrer le nom du compartiment ou le nom du compartiment et le nom du dossier.</p> <p>Par exemple, entrez <code>gs://<nom_compartiment></code> ou <code>gs://<nom_compartiment>/<nom_dossier></code></p>
REGIONID	<p>Nom de région où le jeu de données Google BigQuery se trouve.</p> <p>Pour vous connecter, par exemple, à un jeu de données Google BigQuery qui se trouve dans la région de Las Vegas, spécifiez us-west4 comme ID de région.</p> <p>Remarque: Dans la propriété de connexion Storage Path, veillez à spécifier un nom de compartiment, ou le nom de compartiment et nom de dossier qui se trouvent dans la même région que le jeu de données de Google BigQuery.</p> <p>Pour plus d'informations sur les régions prises en charge par Google BigQuery, consultez la documentation de Google BigQuery suivante : https://cloud.google.com/bigquery/docs/locations</p>

Options de connexion Google Cloud Spanner

Utilisez les options de connexion pour définir la connexion Google Cloud Spanner.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Par exemple :

```
./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"
```

Le tableau suivant décrit les options de connexion Google Cloud Spanner pour les commandes infacmd isp CreateConnection et UpdateConnection :

Propriété	Description
CLIENTEMAIL	Obligatoire. Spécifie la valeur client_email présente dans le fichier JSON que vous téléchargez après avoir créé un compte de service dans Google Cloud Spanner.
PRIVATEKEY	Obligatoire. Spécifie la valeur private_key présente dans le fichier JSON que vous téléchargez après avoir créé un compte de service dans Google Cloud Spanner.
PROJECTID	Obligatoire. Spécifie la valeur project_id présente dans le fichier JSON que vous téléchargez après avoir créé un compte de service dans Google Cloud Spanner. Si vous avez créé plusieurs projets avec le même compte de service, entrez l'ID de projet qui contient le jeu de données auquel vous souhaitez vous connecter.
INSTANCEID	Obligatoire. Nom de l'instance que vous avez créé dans Google Cloud Spanner.

Options de connexion Google Cloud Storage

Utilisez les options de connexion pour définir la connexion Google Cloud Storage.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Par exemple :

```
./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"
```

Le tableau suivant décrit les options de connexion Google Cloud Storage pour les commandes infacmd isp CreateConnection et UpdateConnection :

Propriété	Description
CLIENTEMAIL	Obligatoire. Spécifie la valeur client_email présente dans le fichier JSON que vous téléchargez après avoir créé un compte de service.
PRIVATEKEY	Obligatoire. Spécifie la valeur private_key présente dans le fichier JSON que vous téléchargez après avoir créé un compte de service.
PROJECTID	Obligatoire. Spécifie la valeur project_id présente dans le fichier JSON que vous téléchargez après avoir créé un compte de service. Si vous avez créé plusieurs projets avec le même compte de service, entrez l'ID de projet qui contient le compartiment auquel vous souhaitez vous connecter.

Options de connexion Hadoop

Utilisez les options de connexion pour définir une connexion Hadoop.

Entrez les options de connexion au format suivant :

```
... -o option_name='value' option_name='value' ...
```

Pour entrer plusieurs options, séparez-les par un espace.

Pour entrer des propriétés avancées, utilisez le format suivant :

```
... -o engine_nameAdvancedProperties="'advanced.property.name=value'"
```

Par exemple :

```
... -o blazeAdvancedProperties="'infrgrid.orchestrator.svc.sunset.time=3'"
```

Le tableau suivant décrit les options de connexion Hadoop pour les commandes `infacmd isp` `CreateConnection` et `UpdateConnection` que vous configurez lorsque vous voulez utiliser la connexion Hadoop :

Option	Description
connectionId	Chaîne utilisée par le service d'intégration de données pour identifier la connexion. L'ID n'est pas sensible à la casse. Il peut contenir jusqu'à 255 caractères et doit être unique dans le domaine. Vous ne pouvez pas modifier cette propriété après avoir créé la connexion. La valeur par défaut est le nom de la connexion.
connectionType	Requis. La connexion est de type Hadoop.
nom	Le nom de la connexion. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Vous pouvez modifier cette propriété après avoir créé la connexion. Le nom ne peut pas dépasser 128 caractères, ni contenir des espaces ni les caractères spéciaux suivants : ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /
blazeJobMonitorURL	Nom d'hôte et numéro de port de la surveillance de tâche Blaze. Utiliser le format suivant : <nom d'hôte>:<port> Où - <nom d'hôte> est le nom d'hôte ou l'adresse IP du serveur de surveillance de tâche Blaze. - <port> est le port sur lequel la surveillance de tâche Blaze écoute les appels de procédure distante (RPC). Par exemple, entrez : <code>myhostname:9080</code>
blazeYarnQueueName	Nom de file d'attente du planificateur YARN utilisé par le moteur Blaze qui spécifie les ressources disponibles sur une grappe. Le nom est sensible à la casse.
blazeAdvancedProperties	Propriétés avancées spécifiques au moteur Blaze. Pour entrer plusieurs propriétés, séparez chaque paire nom-valeur avec le texte suivant : <code>&:.</code> N'utilisez les propriétés personnalisées Informatica qu'à la demande du support client international Informatica.
blazeMaxPort	Valeur maximale de la plage de numéros de ports du moteur Blaze. La valeur par défaut est 12600

Option	Description
blazeMinPort	Valeur minimale de la plage de numéros de ports du moteur Blaze. La valeur par défaut est 12300
blazeUserName	Propriétaire du service Blaze et des journaux du service Blaze. Lorsque la grappe Hadoop utilise l'authentification Kerberos, l'utilisateur par défaut est l'utilisateur SPN du service d'intégration de données. Lorsque la grappe Hadoop n'utilise pas l'authentification Kerberos et que l'utilisateur Blaze n'est pas configuré, l'utilisateur par défaut est l'utilisateur du service d'intégration de données.
blazeStagingDirectory	Chemin du fichier HDFS du répertoire que le moteur Blaze utilise pour stocker les fichiers temporaires. Vérifiez que le répertoire existe. Les utilisateurs YARN, du moteur Blaze et de mappage d'emprunt d'identité doivent disposer d'une autorisation d'accès en écriture sur ce répertoire. La valeur par défaut est <code>/blaze/workdir</code> . Si vous désactivez cette propriété, les fichiers intermédiaires sont écrits dans le répertoire intermédiaire Hadoop <code>/tmp/blaze_<nom d'utilisateur></code> .
clusterConfigId	ID de configuration de cluster associé au cluster Hadoop. Vous devez entrer un ID de configuration pour configurer une connexion Hadoop.
hiveStagingDatabaseName	Espace de noms des tables intermédiaires Hive. Utilisez la valeur <code>default</code> du nom pour les tables qui n'ont pas de nom de base de données spécifié.
engineType	Moteur d'exécution des tâches HiveServer2 sur le moteur Spark. La valeur par défaut est MRv2. Vous pouvez choisir MRv2 ou Tez en fonction du type de moteur que la distribution Hadoop utilise : <ul style="list-style-type: none"> - Amazon EMR - Tez - Azure HDI - Tez - Cloudera CDH - MRv2 - Cloudera CDP - Tez - Hortonworks HDP - Tez - MapR - MRv2
environmentSQL	Commandes SQL permettant de définir l'environnement Hadoop. Le service d'intégration de données exécute l'environnement SQL au début de chaque script Hive généré dans un plan d'exécution Hive. Les règles et directives suivantes s'appliquent à l'utilisation de l'environnement SQL : <ul style="list-style-type: none"> - Utilisez l'environnement SQL pour spécifier les demandes Hive. - Utilisez l'environnement SQL pour définir le chemin de classe des fonctions Hive définies par l'utilisateur, puis utilisez l'environnement SQL ou PreSQL pour spécifier les fonctions Hive définies par l'utilisateur. Vous ne pouvez pas utiliser PreSQL dans les propriétés de l'objet de données pour spécifier le chemin de classe. Si vous utilisez les fonctions définies par l'utilisateur Hive, vous devez copier les fichiers <code>.jar</code> dans le répertoire suivant : <code><Informatica installation directory>/services/shared/hadoop/<Hadoop distribution name>/extras/hive-auxjars</code> - Vous pouvez utiliser l'environnement SQL pour définir les paramètres Hadoop ou Hive à utiliser dans les commandes PreSQL ou dans des requêtes personnalisées.

Option	Description
hadoopExecEnvExecutionParameterList	<p>Propriétés personnalisées propres à la connexion Hadoop. Vous pouvez indiquer plusieurs propriétés.</p> <p>Utiliser le format suivant : <code><property>=<value></code></p> <p>Pour spécifier plusieurs propriétés, utilisez & : comme séparateur de propriété.</p> <p>Si plusieurs connexions Hadoop sont associées à la même configuration de grappe, vous pouvez remplacer les valeurs de propriétés définies dans la configuration.</p> <p>N'utilisez les propriétés personnalisées Informatica qu'à la demande du support client international Informatica.</p>
hadoopRejDir	<p>Répertoire distant vers lequel le service d'intégration de données déplace les fichiers de rejet lors de l'exécution de mappages.</p> <p>Activez le répertoire de rejet à l'aide de l'option <code>rejDirOnHadoop</code>.</p>
impersonationUserName	<p>Requis si la grappe Hadoop utilise l'authentification Kerberos. Utilisateur d'emprunt d'identité Hadoop. Nom d'utilisateur emprunté par le service d'intégration de données pour exécuter des mappages dans l'environnement Hadoop.</p> <p>Le service d'intégration de données exécute les mappages en fonction de l'utilisateur configuré. Reportez-vous à l'ordre suivant pour déterminer l'utilisateur dont se sert le service d'intégration de données pour exécuter les mappages :</p> <ol style="list-style-type: none"> 1. Utilisateur du profil de système d'exploitation. Le mappage s'exécute avec l'utilisateur du profil de système d'exploitation si ce dernier est configuré. Si ce n'est pas le cas, le mappage s'exécute avec l'utilisateur d'emprunt d'identité Hadoop. 2. Utilisateur d'emprunt d'identité Hadoop. Le mappage s'exécute avec l'utilisateur d'emprunt d'identité Hadoop si l'utilisateur du profil de système d'exploitation n'est pas configuré. Si l'utilisateur d'emprunt d'identité Hadoop n'est pas configuré, le service d'intégration de données exécute les mappages avec l'utilisateur du service d'intégration de données. 3. Utilisateur du service d'intégration de données. Le mappage s'exécute avec l'utilisateur du service d'intégration de données si l'utilisateur du profil du système d'exploitation et l'utilisateur d'emprunt d'identité Hadoop ne sont pas configurés.
hiveWarehouseDirectoryOnHDFS	<p>Facultatif. Chemin de fichier HDFS absolu de la base de données par défaut pour l'entrepôt local associé à la grappe.</p> <p>Si vous ne configurez pas le répertoire de l'entrepôt Hive, le moteur Hive essaie d'abord d'écrire dans le répertoire spécifié dans la propriété de configuration de grappe <code>hive.metastore.warehouse.dir</code>. Si la configuration de grappe ne possède pas la propriété, le moteur Hive écrit dans le répertoire par défaut / <code>user/hive/warehouse</code>.</p>
metastoreDatabaseDriver	<p>Nom de classe du pilote pour le magasin de données JDBC. Par exemple, le nom de classe suivant indique un pilote MySQL :</p> <pre>com.mysql.jdbc.Driver</pre> <p>Vous pouvez obtenir la valeur du pilote de base de données du magasin de métadonnées à partir du fichier <code>hive-site.xml</code>. Le pilote de base de données du magasin de métadonnées s'affiche comme la propriété suivante dans le fichier <code>hive-site.xml</code> :</p> <pre><property> <name>javax.jdo.option.ConnectionDriverName</name> <value>com.mysql.jdbc.Driver</value> </property></pre>

Option	Description
metastoreDatabasePassword	<p>Mot de passe du nom d'utilisateur du magasin de métadonnées.</p> <p>Vous pouvez obtenir la valeur du mot de passe de base de données du magasin de métadonnées à partir du fichier hive-site.xml. Le mot de passe de base de données du magasin de métadonnées s'affiche comme la propriété suivante dans le fichier hive-site.xml:</p> <pre><property> <name>javax.jdo.option.ConnectionPassword</name> <value>password</value> </property></pre>
metastoreDatabaseURI	<p>URI de la connexion JDBC utilisé pour accéder au magasin de données dans une configuration de magasin de métadonnées local. Utilisez l'URI de connexion suivante :</p> <pre>jdbc:<datastore type>://<node name>:<port>/<database name></pre> <p>où</p> <ul style="list-style-type: none"> - <node name> est le nom d'hôte ou l'adresse IP du magasin de données. - <data store type> est le type de magasin de données. - <port> est le port sur lequel le magasin de données écoute les appels de procédure distante (RPC). - <database name> est le nom de la base de données. <p>Par exemple, l'URI suivant spécifie un magasin de métadonnées local qui utilise MySQL comme magasin de données :</p> <pre>jdbc:mysql://hostname23:3306/metastore</pre> <p>Vous pouvez obtenir la valeur de l'URI de la base de données du magasin de métadonnées à partir du fichier hive-site.xml. L'URI de la base de données du magasin de métadonnées s'affiche comme la propriété suivante dans le fichier hive-site.xml :</p> <pre><property> <name>javax.jdo.option.ConnectionURL</name> <value>jdbc:mysql://MYHOST/metastore</value> </property></pre>
metastoreDatabaseUserName	<p>Nom d'utilisateur de la base de données du magasin de métadonnées.</p> <p>Vous pouvez obtenir la valeur du nom d'utilisateur de la base de données du magasin de métadonnées à partir du fichier hive-site.xml. Le nom d'utilisateur de la base de données du magasin de métadonnées s'affiche comme la propriété suivante dans le fichier hive-site.xml :</p> <pre><property> <name>javax.jdo.option.ConnectionUserName</name> <value>hiveuser</value> </property></pre>

Option	Description
metastoreMode	<p>Détermine s'il faut se connecter au magasin de métadonnées distant ou local. Par défaut, le magasin de métadonnées local est sélectionné. Pour un magasin de métadonnées local, vous devez indiquer l'URI et le pilote de la base de données du magasin de métadonnées, le nom d'utilisateur et le mot de passe. Pour un magasin de métadonnées distant, vous devez uniquement indiquer l'URI du magasin de métadonnées distant.</p> <p>Vous pouvez obtenir la valeur du mode d'exécution du magasin de métadonnées à partir du fichier hive-site.xml. Le mode d'exécution du magasin de métadonnées s'affiche comme la propriété suivante dans le fichier hive-site.xml :</p> <pre><property> <name>hive.metastore.local</name> <value>true</true> </property></pre> <p>Remarque: La propriété <code>hive.metastore.local</code> est obsolète dans le fichier <code>hive-site.xml</code> pour les versions du serveur Hive 0.9 et supérieures. Si la propriété <code>hive.metastore.local</code> n'existe pas, mais que la propriété <code>hive.metastore.uris</code> existe et que vous savez que le serveur Hive a démarré, vous pouvez définir la connexion sur un magasin de métadonnées distant.</p>
remoteMetastoreURI	<p>URI du magasin de métadonnées utilisé pour accéder aux métadonnées dans une configuration distante de magasin de métadonnées. Pour un magasin de métadonnées distant, vous devez indiquer les détails du serveur Thrift.</p> <p>Utilisez l'URI de connexion suivante :</p> <pre>thrift://<hostname>:<port></pre> <p>Où</p> <ul style="list-style-type: none"> - <code><nom d'hôte></code> est le nom ou l'adresse IP du serveur de magasins de métadonnées Thrift. - <code><port></code> est le port sur lequel le serveur Thrift écoute. <p>Par exemple, entrez : <code>thrift://myhostname:9083/</code></p> <p>Vous pouvez obtenir la valeur de l'URI du magasin de métadonnées distant à partir du fichier <code>hive-site.xml</code>. L'URI du magasin de métadonnées distant s'affiche comme la propriété suivante dans le fichier <code>hive-site.xml</code> :</p> <pre><property> <name>hive.metastore.uris</name> <value>thrift://<n.n.n.n>:9083</value> <description> IP address or fully-qualified domain name and port of the metastore host</description> </property></pre>
rejDirOnHadoop	<p>Active <code>hadoopRejDir</code>. Permet de spécifier l'emplacement vers lequel déplacer les fichiers de rejet lors de l'exécution de mappages.</p> <p>Si cette option est activée, le service d'intégration de données déplace les fichiers de mappage vers l'emplacement HDFS répertorié dans <code>hadoopRejDir</code>.</p> <p>Par défaut, le service d'intégration de données stocke les fichiers de mappage en fonction du paramètre système <code>RejectDir</code>.</p>
sparkEventLogDir	<p>Facultatif. Chemin du fichier HDFS du répertoire que le moteur Spark utilise pour journaliser les événements.</p>
sparkAdvancedProperties	<p>Propriétés avancées spécifiques au moteur Spark.</p> <p>Pour entrer plusieurs propriétés, séparez chaque paire nom-valeur avec le texte suivant : <code>& ;</code>.</p> <p>N'utilisez les propriétés personnalisées Informatica qu'à la demande du support client international Informatica.</p>

Option	Description
sparkStagingDirectory	Chemin du fichier HDFS du répertoire que le moteur Spark utilise pour stocker les fichiers temporaires d'exécution des tâches. Les utilisateurs YARN, du service d'intégration de données et du mappage d'emprunt d'identité doivent disposer d'une autorisation d'accès en écriture sur ce répertoire. Par défaut, les fichiers temporaires sont écrits dans le répertoire intermédiaire Hadoop /tmp/spark_<nom d'utilisateur>.
sparkYarnQueueName	Nom de la file d'attente du planificateur YARN utilisé par le moteur Spark qui spécifie les ressources disponibles sur une grappe. Le nom est sensible à la casse.
stgDataCompressionCodecClasses	Nom de classe de codec qui active la compression des données et améliore les performances dans les tables intermédiaires temporaires. Le nom de la classe de codec correspond au type de code.
stgDataCompressionCodecType	Bibliothèque de compression Hadoop pour un nom de classe de codec de compression. Vous pouvez choisir Aucun, Zlib, Gzip, Snappy, Bz2, LZO ou Personnalisé. La valeur par défaut est Aucun.

Options de connexion HBase

Utilisez des options de connexion pour définir une connexion HBase. Vous pouvez utiliser une connexion HBase pour vous connecter à une table HBase ou à une table MapR-DB.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion HBase pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
DATABASETYPE	Requis lorsque vous créez une connexion HBase pour une table MapR-DB. Définissez la valeur sur MapR-DB. La valeur par défaut est HBase.
clusterConfigId	ID de configuration de cluster associé au cluster Hadoop. Vous devez entrer un ID de configuration pour configurer une connexion Hadoop.
maprdbpath	Requis si vous créez une connexion HBase pour vous connecter à une table MapR-DB. Définissez la valeur sur le chemin de la base de données qui contient la table MapR-DB à laquelle vous souhaitez vous connecter. Entrez un chemin d'accès de grappe MapR valide. Placez la valeur entre guillemets simples. Lorsque vous créez un objet de données HBase pour MapR-DB, vous pouvez parcourir uniquement les tables qui existent dans le chemin d'accès spécifié dans cette option. Vous ne pouvez pas accéder aux tables qui sont disponibles dans les sous-répertoires dans le chemin d'accès spécifié. Par exemple, si vous spécifiez maprdbpath en tant que /user/Customers/, vous pouvez accéder aux tables dans le répertoire Customers. Toutefois, si le répertoire Customers contient un sous-répertoire nommé Regions, vous ne pouvez pas accéder aux tables du répertoire suivant : /user/customers/regions

Options de connexion HDFS

Utilisez les options de connexion pour définir une connexion HDFS.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion HDFS pour les commandes `infacmd isp CreateConnection` et `UpdateConnection` :

Option	Description
userName	Nom d'utilisateur pour accéder à HDFS.
nameNodeURI	URI d'accès au système de stockage. La valeur <code>fs.defaultFS</code> se trouve dans l'ensemble de configuration <code>core-site.xml</code> de la configuration de la grappe.
clusterConfigId	ID de configuration de cluster associé au cluster Hadoop. Vous devez entrer un ID de configuration pour configurer une connexion Hadoop.

Options de connexion Hive

Utilisez les options de connexion pour définir une connexion Hive.

Entrez les options de connexion au format suivant :

```
... -o option_name='value' option_name='value' ...
```

Pour entrer plusieurs options, séparez-les par un espace.

Le tableau suivant décrit les options de connexion Hive pour les commandes `infacmd isp CreateConnection` et `UpdateConnection` que vous configurez lorsque vous voulez utiliser la connexion Hive :

Option	Description
connectionType	Obligatoire. La connexion est de type Hive.
name	Le nom de la connexion. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Vous pouvez modifier cette propriété après avoir créé la connexion. Le nom ne peut pas dépasser 128 caractères, ni contenir des espaces ni les caractères spéciaux suivants : ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /

Option	Description
environmentSQL	<p>Commandes SQL permettant de définir l'environnement Hadoop. Dans un environnement de type natif, le service d'intégration de données exécute l'environnement SQL chaque fois qu'il crée une connexion vers le magasin de métadonnées Hive. Si la connexion Hive est utilisée pour exécuter les mappages dans la grappe Hadoop, le service d'intégration de données exécute l'environnement SQL au début de chaque session Hive.</p> <p>Les règles et directives suivantes s'appliquent à l'utilisation de l'environnement SQL dans les deux modes de connexion :</p> <ul style="list-style-type: none"> - Utilisez l'environnement SQL pour spécifier les demandes Hive. - Utilisez l'environnement SQL pour définir le chemin de classe des fonctions Hive définies par l'utilisateur, puis utilisez un environnement SQL ou PreSQL pour spécifier les fonctions Hive définies par l'utilisateur. Vous ne pouvez pas utiliser PreSQL dans les propriétés de l'objet de données pour spécifier le chemin de classe. Si vous utilisez des fonctions définies par l'utilisateur Hive, vous devez copier les fichiers .jar dans le répertoire suivant : <pre><Informatica installation directory>/services/shared/hadoop/ <Hadoop distribution name>/extras/hive-auxjars</pre> - Vous pouvez également utiliser un environnement SQL pour définir les paramètres Hadoop ou Hive que vous comptez utiliser dans les commandes PreSQL ou dans des demandes personnalisées. <p>Si la connexion Hive est utilisée pour exécuter les mappages dans la grappe Hadoop, seul l'environnement SQL de la connexion Hive est exécuté. Les différentes commandes de l'environnement SQL pour les connexions de la source ou de la cible Hive ne sont pas exécutées, même si les sources et les cibles Hive se trouvent sur différentes grappes.</p>
quoteChar	<p>Type de caractère servant à identifier les caractères spéciaux et les mots clés SQL réservés, tels que WHERE. Le service d'intégration de données place le caractère sélectionné autour des caractères spéciaux et des mots clés SQL réservés. Le service d'intégration de données utilise également ce caractère pour la propriété Prise en charge des identifiants à casse mixte.</p>
clusterConfigId	<p>ID de configuration de cluster associé au cluster Hadoop. Vous devez entrer un ID de configuration pour configurer une connexion Hadoop.</p>

Propriétés pour accéder à Hive en tant que source ou cible

Le tableau suivant décrit les options obligatoires pour les commandes `infacmd isp CreateConnection` et `UpdateConnection` que vous configurez lorsque vous voulez utiliser la connexion Hive pour accéder aux données Hive :

Propriété	Description
<code>hiveJdbcDriverClassName</code>	Nom de classe du pilote JDBC.
<code>metadataConnString</code>	<p>URI de la connexion JDBC utilisée pour accéder aux métadonnées depuis le serveur Hadoop.</p> <p>La chaîne de connexion utilise le format suivant :</p> <pre>jdbc:hive://<hostname>:<port>/<db></pre> <p>Où</p> <ul style="list-style-type: none">- <code>hostname</code> est le nom ou l'adresse IP de l'ordinateur sur laquelle le serveur Hive est exécuté.- <code>port</code> est le port sur lequel le serveur Hive écoute.- <code>db</code> est la base de données à laquelle vous voulez vous connecter. Si vous ne fournissez pas les détails de la base de données, le service d'intégration de données utilise les détails par défaut. <p>Pour se connecter à HiveServer 2, utilisez le format de chaîne de connexion implémenté par Apache Hive pour cette distribution Hadoop spécifique. Pour plus d'informations sur les formats de chaîne de connexion Apache Hive, consultez la documentation Apache Hive.</p> <p>Si le groupe Hadoop utilise l'authentification SSL ou TLS, vous devez ajouter <code>ssl = true</code> à l'URI de connexion JDBC. Par exemple : <code>jdbc:hive2://<hostname>:<port>/<db>;ssl=true</code></p> <p>Si vous utilisez un certificat auto-signé pour l'authentification SSL ou TLS, assurez-vous que le fichier de certificat est disponible sur la machine cliente et celle du service d'intégration de données. Pour plus d'informations, consultez le document <i>Informatica Big Data Management Cluster Integration Guide</i>.</p>
<code>bypassHiveJDBCServer</code>	<p>Mode de pilote JDBC. Activez cette option pour utiliser le pilote JDBC intégré (en mode intégré).</p> <p>Pour utiliser le mode intégré de JDBC, procédez comme suit :</p> <ul style="list-style-type: none">- Vérifiez que le client Hive et les services Informatica sont installés sur le même ordinateur.- Configurez les propriétés de la connexion Hive pour exécuter les mappages dans la grappe Hadoop. <p>Si vous choisissez le mode non intégré, vous devez configurer la chaîne de connexion d'accès aux données.</p> <p>Le mode intégré JDBC est préférable au mode non intégré.</p>

Propriété	Description
sqlAuthorized	<p>Lorsque vous sélectionnez l'option pour observer l'authentification SQL à grain fin dans une source Hive, le mappage observe les restrictions au niveau des lignes et des colonnes de l'accès aux données. Si vous ne sélectionnez pas cette option, le moteur d'exécution Blaze ignore les restrictions et les résultats incluent des données restreintes.</p> <p>Applicable aux grappes Hadoop sur lesquelles les modes de sécurité Sentry ou Ranger sont activés.</p>
connectString	<p>La chaîne de connexion utilisée pour accéder aux données depuis le stockage de données Hadoop. La chaîne de connexion du mode JDBC non intégré doit être au format suivant :</p> <pre>jdbc:hive://<hostname>:<port>/<db></pre> <p>Où</p> <ul style="list-style-type: none"> - <code>hostname</code> est le nom ou l'adresse IP de l'ordinateur sur laquelle le serveur Hive est exécuté. - <code>port</code> est le port sur lequel le serveur Hive écoute. La valeur par défaut est 10 000. - <code>db</code> est la base de données à laquelle vous voulez vous connecter. Si vous ne fournissez pas les détails de la base de données, le service d'intégration de données utilise les détails par défaut. <p>Pour se connecter à HiveServer 2, utilisez le format de chaîne de connexion implémenté par Apache Hive pour cette distribution Hadoop spécifique. Pour plus d'informations sur les formats de chaîne de connexion Apache Hive, consultez la documentation Apache Hive.</p> <p>Si le groupe Hadoop utilise l'authentification SSL ou TLS, vous devez ajouter <code>ssl = true</code> à l'URI de connexion JDBC. Par exemple : <code>jdbc:hive2://<hostname>:<port>/<db>;ssl=true</code></p> <p>Si vous utilisez un certificat auto-signé pour l'authentification SSL ou TLS, assurez-vous que le fichier de certificat est disponible sur la machine cliente et celle du service d'intégration de données. Pour plus d'informations, consultez le document <i>Informatica Big Data Management Cluster Integration Guide</i>.</p>

Propriétés pour exécuter des mappages dans la grappe Hadoop

Le tableau suivant décrit les options obligatoires pour les commandes `infacmd isp CreateConnection` et `UpdateConnection` que vous configurez lorsque vous voulez utiliser la connexion Hive pour exécuter des mappages Informatica dans la grappe Hadoop :

Propriété	Description
databaseName	Espace de nom pour les tables. Utilisez la valeur <code>default</code> du nom pour les tables qui n'ont pas de nom de base de données spécifié.
customProperties	<p>Configure ou remplace les propriétés de grappe Hive ou Hadoop dans le fichier de configuration <code>hive-site.xml</code> défini sur la machine sur laquelle s'exécute le service d'intégration de données. Vous pouvez indiquer plusieurs propriétés.</p> <p>Sélectionnez Modifier pour spécifier le nom et la valeur de la propriété. La propriété s'affiche selon le format suivant :</p> <pre><property1>=<value></pre> <p>Lorsque vous spécifiez plusieurs propriétés, <code>&</code> : s'affiche comme séparateur de propriété.</p> <p>La longueur maximale du format est de 1 Mo.</p> <p>Si vous entrez une propriété requise pour une connexion Hive, elle remplace la propriété que vous configurez dans les propriétés Hive/Hadoop avancées.</p> <p>Le service d'intégration de données ajoute ou définit ces propriétés pour chaque tâche MapReduce. Vous pouvez vérifier ces propriétés dans le JobConf de chaque tâche MapReduce. Accédez au JobConf de chaque tâche depuis l'URL Jobtracker sous chaque tâche MapReduce.</p> <p>Le service d'intégration de données écrit des messages pour ces propriétés dans les journaux du service d'intégration de données. Le service d'intégration de données doit avoir le niveau de traçage des journaux défini pour journaliser chaque ligne ou défini pour le traçage d'initialisation détaillée.</p> <p>Par exemple, indiquez les propriétés suivantes pour contrôler et limiter le nombre de réducteurs pour exécuter une tâche de mappage :</p> <pre>mapred.reduce.tasks=2&hive.exec.reducers.max=10</pre>
stgDataCompressionCodecClass	Nom de classe de codec qui active la compression des données et améliore les performances dans les tables intermédiaires temporaires. Le nom de la classe de codec correspond au type de code.
stgDataCompressionCodecType	<p>Bibliothèque de compression Hadoop pour un nom de classe de codec de compression.</p> <p>Vous pouvez choisir Aucun, Zlib, Gzip, Snappy, Bz2, LZ0 ou Personnalisé.</p> <p>La valeur par défaut est Aucun.</p>

Options de connexion IBM DB2

Utilisez les options de connexion pour définir une connexion IBM DB2.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion IBM DB2 pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
PassThruEnabled	Facultatif. Active la sécurité des intercommunications de la connexion. Lorsque vous activez la sécurité des intercommunications d'une connexion, le domaine utilise le nom d'utilisateur et le mot de passe du client au lieu des justificatifs d'identité définis dans l'objet de connexion pour se connecter à la base de données correspondante.
MetadataAccessConnect String	<p>Requis. URL de connexion JDBC utilisée pour accéder aux métadonnées de la base de données.</p> <pre>jdbc:informatica:db2://<nom d'hôte>:<port>;DatabaseName=<nom de la base de données></pre> <p>Lorsque vous importez une table depuis l'outil Developer tool ou l'outil Analyst tool, par défaut, toutes les tables sont affichées dans le nom de schéma par défaut. Pour afficher les tables dans un schéma spécifique au lieu du schéma par défaut, vous pouvez spécifier le nom du schéma à partir duquel vous voulez importer la table. Incluez le paramètre ischename dans l'URL afin de spécifier le nom de schéma. Par exemple, utilisez la syntaxe suivante pour importer une table à partir d'un schéma spécifique :</p> <pre>jdbc:informatica:db2://<nom d'hôte>:<port>;DatabaseName=<nom de la base de données>;ischename=<schema_name></pre> <p>Pour rechercher une table dans plusieurs schémas et l'importer, vous pouvez spécifier plusieurs noms de schéma dans le paramètre ischename. Le nom de schéma est sensible à la casse. Vous ne pouvez pas utiliser des caractères spéciaux lorsque vous spécifiez plusieurs noms de schéma. La barre verticale () vous permet de séparer plusieurs noms de schémas. Par exemple, utilisez la syntaxe suivante pour rechercher une table dans trois schémas et l'importer :</p> <pre>jdbc:informatica:db2://<nom d'hôte>:<port>;DatabaseName=<nom de la base de données>;ischename=<schema_name1> <schema_name2> <schema_name3></pre>

Option	Description
AdvancedJDBCSecurityOptions	<p>Facultatif. Paramètres de base de données pour l'accès aux métadonnées d'une base de données sécurisée. Informatica traite la valeur du champ AdvancedJDBCSecurityOptions comme des données sensibles et crypte la chaîne de paramètres.</p> <p>Pour vous connecter à une base de données sécurisée, incluez les paramètres suivants :</p> <ul style="list-style-type: none"> - EncryptionMethod. Requis. Indique si les données sont cryptées lorsqu'elles sont transmises sur le réseau. Ce paramètre doit être défini pour SSL. - ValidateServerCertificate. Facultatif. Indique si Informatica valide le certificat envoyé par le serveur de base de données. <p>Si ce paramètre est défini sur True, Informatica valide le certificat envoyé par le serveur de base de données. Si vous spécifiez le paramètre HostNameInCertificate, Informatica valide également le nom d'hôte dans le certificat.</p> <p>Si ce paramètre est défini sur false, Informatica ne valide pas le certificat envoyé par le serveur de base de données. Informatica ignore les informations de truststore que vous spécifiez.</p> <ul style="list-style-type: none"> - HostNameInCertificate. Facultatif. Nom d'hôte de la machine qui héberge la base de données sécurisée. Si vous spécifiez un nom d'hôte, Informatica valide le nom d'hôte inclus dans la chaîne de connexion avec le nom d'hôte dans le certificat SSL. - TrustStore. Requis. Chemin et nom du fichier truststore contenant le certificat SSL de la base de données. - TrustStorePassword. Requis. Mot de passe du fichier truststore de la base de données sécurisée. <p>Remarque: Pour obtenir la liste complète des paramètres JDBC sécurisés, consultez la documentation de DataDirect JDBC.</p> <p>Informatica ajoute les paramètres JDBC sécurisés à la chaîne de connexion. Si vous incluez les paramètres JDBC sécurisés directement dans la chaîne de connexion, n'entrez aucun paramètre dans le champ AdvancedJDBCSecurityOptions.</p>
DataAccessConnectionString	<p>Chaîne de connexion utilisée pour accéder aux données de la base de données.</p> <p>Entrez la chaîne de connexion au format suivant :</p> <p><nom de base de données></p>
CodePage	<p>Requis. Page de code utilisée pour lire une base de données source ou écrire dans une base de données cible.</p>
EnvironmentSQL	<p>Facultatif. Commandes SQL permettant de définir l'environnement de base de données lorsque vous vous connectez à la base de données. Le service d'intégration de données exécute le SQL de l'environnement de connexion à chaque connexion à la base de données.</p> <p>Par exemple, ALTER SESSION SET CURRENT_SCHEMA=INFA_USR;</p> <p>Remarque: Placez les caractères spéciaux entre guillemets doubles.</p>
TransactionSQL	<p>Facultatif. Commandes SQL à exécuter avant chaque transaction. Le service d'intégration de données exécute le SQL transactionnel au début de chaque transaction.</p> <p>Par exemple, SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;</p> <p>Remarque: Placez les caractères spéciaux entre guillemets doubles.</p>
Espace de table	<p>Facultatif. Nom de l'espace de table de la base de données.</p>

Option	Description
QuoteChar	Facultatif. Caractère que vous utiliserez pour les guillemets dans cette connexion. Type de caractère servant à identifier les caractères spéciaux et les mots clés SQL réservés, tels que WHERE. Le service d'intégration de données place le caractère sélectionné autour des caractères spéciaux et des mots clés SQL réservés. Le service d'intégration de données utilise également ce caractère pour la propriété QuoteChar. La valeur par défaut est 0.
EnableQuotes	Facultatif. Sélectionnez cette option pour activer les guillemets pour cette connexion. Lorsque cette option est activée, le service d'intégration de données place les caractères identifiants autour des noms de table, de vue, de schéma, de synonyme et de colonne lors de la génération et de l'exécution de SQL par rapport à ces objets dans la connexion. Utilisez-la si les objets comportent une casse mixte ou des noms en minuscules. Les valeurs valides sont True ou False. La valeur par défaut est True.
EnableConnectionPool	Facultatif. Active le pooling de connexions. Lorsque vous activez le pooling de connexions, celui-ci conserve les instances de connexion inactives en mémoire. Lorsque vous désactivez le pooling de connexions, le service d'intégration de données arrête toute l'activité du pooling. Les valeurs valides sont True ou False. La valeur par défaut est True.
ConnectionPoolSize	Facultatif. Nombre maximal d'instances de connexion inactives que le service d'intégration de données gère pour une connexion de base de données. Définissez cette valeur à une valeur supérieure au nombre minimal d'instances de connexion inactives. La valeur par défaut est 15.
ConnectionPoolMaxIdleTime	Facultatif. Nombre de secondes pendant lesquelles une connexion qui dépasse le nombre minimal d'instances de connexion peut rester inactive avant que le pool de connexions ne l'abandonne. Le pool de connexions ignore la durée d'inactivité lorsque celle-ci ne dépasse pas le nombre minimal d'instances de connexion inactives. La valeur par défaut est 120.
ConnectionPoolMinConnections	Facultatif. Nombre minimal d'instances de connexion inactives que le pool maintient pour une connexion de base de données. Définissez cette valeur comme étant égale ou inférieure à la taille du pool de connexions inactives. La valeur par défaut est 0.

Options de connexion IMS

Utilisez les options de connexion pour définir une connexion IMS.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion IMS :

Option	Description
CodePage	Requis. Code devant être lu dans la base de données ou écrit dans celle-ci. Utilisez le nom de la page du code ISO, par exemple ISO-8859-6. Le nom de la page du code n'est pas sensible à la casse.
ArraySize	Facultatif. Détermine le nombre d'enregistrements dans la matrice de stockage pour les threads lorsque la valeur des threads de travail est supérieure à 0. Les valeurs valides sont comprises entre 1 et 5 000. La valeur par défaut est 25.
Compression	Facultatif. Compresse les données pour réduire le volume de données que les applications Informatica écrivent sur le réseau. True ou false. La valeur par défaut est False.
EncryptionLevel	Facultatif. Niveau de chiffrement. Si vous spécifiez AES pour l'option EncryptionType, spécifiez l'une des valeurs suivantes pour indiquer le niveau de chiffrement AES : <ul style="list-style-type: none"> - 1. Utilisez une clé de chiffrement 128 bits. - 2. Utilisez une clé de chiffrement 192 bits. - 3. Utilisez une clé de chiffrement 256 bits. La valeur par défaut est 1. Remarque: Si vous sélectionnez Aucun pour le type de chiffrement, le service d'intégration de données ignore la valeur de niveau de chiffrement.
EncryptionType	Facultatif. Vérifie s'il faut utiliser le chiffrement. Spécifiez l'une des valeurs suivantes : <ul style="list-style-type: none"> - Aucun - AES La valeur par défaut est Aucun.
InterpretAsRows	Facultatif. Si la valeur est « Vrai », la taille de stimulation représente un nombre de lignes. Si la valeur est False, la taille de stimulation représente des kilooctets. La valeur par défaut est False.
Emplacement	Emplacement du nœud Écouteur PowerExchange qui peut se connecter à la base de données. L'emplacement est défini dans le premier paramètre de l'instruction NODE dans le fichier de configuration dbmover.cfg de PowerExchange.
OffLoadProcessing	Facultatif. Déplace le traitement des données en bloc depuis la machine source vers la machine du service d'intégration de données. Entrez l'une des valeurs suivantes : <ul style="list-style-type: none"> - Auto. Le service d'intégration de données détermine si vous souhaitez utiliser le traitement de déchargement. - Oui. Utiliser le traitement de déchargement. - Non. Ne pas utiliser le traitement de déchargement. La valeur par défaut est Auto.
PacingSize	Facultatif. Ralentit le taux de transfert de données pour réduire les goulots d'étranglement. Plus la valeur est basse, plus les performances de la session sont élevées. La valeur minimale est 0. Entrez 0 pour des performances optimales. La valeur par défaut est 0.
WorkerThread	Facultatif. Nombre de threads que le service d'intégration de données utilise pour traiter les données en bloc lorsque le traitement du déchargement est activé. Pour des performances optimales, cette valeur ne doit pas dépasser le nombre de processeurs disponibles sur la machine du service d'intégration de données. Les valeurs valides vont de 1 à 64. La valeur par défaut est 0, ce qui désactive le multithreading.

Option	Description
WriteMode	Entrez l'un des modes d'écriture suivants : <ul style="list-style-type: none"> - CONFIRMWRITEON. Envoie des données à l'Écouteur PowerExchange et attend la réponse de réussite/échec avant d'envoyer davantage de données. - CONFIRMWRITEOFF. Envoie des données à l'Écouteur PowerExchange sans attendre la réponse de réussite/échec. Utilisez cette option lorsque la table cible peut être rechargée si une erreur se produit. - ASYNCHRONOUSWITHFAULTT. Envoie des données à l'Écouteur PowerExchange de manière asynchrone avec la possibilité de détecter les erreurs. La valeur par défaut est CONFIRMWRITEON.
EnableConnectionPool	Facultatif. Active le pooling de connexions. Lorsque vous activez le pooling de connexions, celui-ci conserve les instances de connexion inactives en mémoire. Lorsque vous désactivez le pooling de connexions, le service d'intégration de données arrête toute l'activité du pooling. True ou false. La valeur par défaut est False.
ConnectionPoolSize	Facultatif. Nombre maximal d'instances de connexion inactives que le service d'intégration de données gère pour une connexion de base de données. Définissez cette valeur à une valeur supérieure au nombre minimal d'instances de connexion inactives. La valeur par défaut est 15.
ConnectionPoolMaxIdleTime	Facultatif. Nombre de secondes pendant lesquelles une connexion qui dépasse le nombre minimal d'instances de connexion peut rester inactive avant que le pool de connexions ne l'abandonne. Le pool de connexions ignore la durée d'inactivité lorsque celle-ci ne dépasse pas le nombre minimal d'instances de connexion inactives. La valeur par défaut est 120.
ConnectionPoolMinConnections	Facultatif. Nombre minimal d'instances de connexion inactives que le pool maintient pour une connexion de base de données. Définissez cette valeur comme étant égale ou inférieure à la taille du pool de connexions inactives. La valeur par défaut est 0.

Options de connexion JDBC

Utilisez les options de connexion pour définir une connexion JDBC.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par des espaces. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion JDBC pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
JDBCClassName	<p>Classe Java à utiliser pour vous la connexion à la base de données.</p> <p>La liste suivante fournit le nom de classe du pilote que vous pouvez entrer pour le type de base de données concerné :</p> <ul style="list-style-type: none"> - Nom de classe du pilote DataDirect JDBC pour Oracle : com.informatica.jdbc.oracle.OracleDriver - Nom de classe du pilote DataDirect JDBC pour IBM DB2 : com.informatica.jdbc.db2.DB2Driver - Nom de classe du pilote DataDirect JDBC pour Microsoft SQL Server : com.informatica.jdbc.sqlserver.SQLServerDriver - Nom de classe du pilote DataDirect JDBC pour Sybase ASE : com.informatica.jdbc.sybase.SybaseDriver - Nom de classe du pilote DataDirect JDBC pour Informix : com.informatica.jdbc.informix.InformixDriver - Nom de classe du pilote DataDirect JDBC pour MySQL : com.informatica.jdbc.mysql.MySQLDriver <p>Pour plus d'informations sur la classe de pilote à utiliser avec des bases de données spécifiques, consultez la documentation du fournisseur.</p>
MetadataConnString	<p>URL utilisée pour vous la connexion à la base de données.</p> <p>La liste suivante fournit la chaîne de connexion que vous pouvez entrer pour le type de base de données concerné :</p> <ul style="list-style-type: none"> - Pilote DataDirect JDBC pour Oracle : jdbc:informatica:oracle://<hostname>:<port>;SID=<sid> - Pilote DataDirect JDBC pour IBM DB2 : jdbc:informatica:db2://<hostname>:<port>;DatabaseName=<database name> - Pilote DataDirect JDBC pour Microsoft SQL Server : jdbc:informatica:sqlserver://<host>:<port>;DatabaseName=<database name> - Pilote DataDirect JDBC pour Sybase ASE : jdbc:informatica:sybase://<host>:<port>;DatabaseName=<database name> - Pilote DataDirect JDBC pour Informix : jdbc:informatica:informix://<host>:<port>;informixServer=<informix server name>;databaseName=<dbName> - Pilote DataDirect JDBC pour MySQL : jdbc:informatica:mysql://<host>:<port>;DatabaseName=<database name> <p>Pour plus d'informations sur la chaîne de connexion à utiliser pour des bases de données spécifiques, consultez la documentation du fournisseur pour la syntaxe de l'URL.</p>
EnvironmentSQL	<p>Facultatif. Commandes SQL permettant de définir l'environnement de base de données lorsque vous vous connectez à la base de données. Le service d'intégration de données exécute le SQL de l'environnement de connexion à chaque connexion à la base de données.</p> <p>Par exemple, ALTER SESSION SET CURRENT_SCHEMA=INFA_USR;</p> <p>Remarque: Placez les caractères spéciaux entre guillemets doubles.</p>
TransactionSQL	<p>Facultatif. Commandes SQL à exécuter avant chaque transaction. Le service d'intégration de données exécute le SQL transactionnel au début de chaque transaction.</p> <p>Par exemple, SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;</p> <p>Remarque: Placez les caractères spéciaux entre guillemets doubles.</p>

Option	Description
QuoteChar	Facultatif. Caractère que vous utiliserez pour les guillemets dans cette connexion. Type de caractère servant à identifier les caractères spéciaux et les mots clés SQL réservés, tels que WHERE. Le service d'intégration de données place le caractère sélectionné autour des caractères spéciaux et des mots clés SQL réservés. Le service d'intégration de données utilise également ce caractère pour la propriété QuoteChar. La valeur par défaut est DOUBLE_QUOTE.
EnableQuotes	Facultatif. Sélectionnez cette option pour activer les guillemets pour cette connexion. Lorsque cette option est activée, le service d'intégration de données place les caractères identifiants autour des noms de table, de vue, de schéma, de synonyme et de colonne lors de la génération et de l'exécution de SQL par rapport à ces objets dans la connexion. Utilisez-la si les objets comportent une casse mixte ou des noms en minuscules. Les valeurs valides sont True ou False. La valeur par défaut est True.
hadoopConnector	Obligatoire si vous souhaitez activer la connectivité Sqoop pour l'objet de données qui utilise la connexion JDBC. Le service d'intégration de données exécute le mappage dans l'environnement d'exécution Hadoop via Sqoop. Vous pouvez configurer la connectivité Sqoop pour des objets de données relationnels, des objets de données personnalisés et des objets de données logiques qui sont basés sur une base de données compatible avec JDBC. Définissez la valeur sur <code>SQOOP_146</code> pour activer la connectivité Sqoop.
hadoopConnectorArgs	Facultatif. Entrez les arguments que le programme Sqoop doit utiliser pour se connecter à la base de données. Placez les arguments Sqoop entre guillemets simples. Séparez les arguments multiples par un espace. Par exemple, <code>hadoopConnectorArgs='--<Sqoop argument 1> --<Sqoop argument 2>'</code> Pour lire des données depuis Teradata ou écrire des données dans Teradata par l'intermédiaire de connecteurs spécialisés TDCH (connecteur Teradata pour Hadoop) pour Sqoop, définissez la classe de fabrique de la connexion TDCH dans l'argument <code>hadoopConnectorArgs</code> . La classe de fabrique de la connexion dépend du connecteur Sqoop TDCH que vous souhaitez utiliser. <ul style="list-style-type: none"> - Pour utiliser Cloudera Connector fourni par Teradata, configurez l'argument <code>hadoopConnectorArgs</code> de la manière suivante : <pre>hadoopConnectorArgs='- Dsqaop.connection.factories=com.cloudera.connector.teradata.Teradata ManagerFactory'</pre> - Pour utiliser Hortonworks Connector for Teradata (fourni par Teradata Connector for Hadoop), configurez l'argument <code>hadoopConnectorArgs</code> de la manière suivante : <pre>hadoopConnectorArgs='- Dsqaop.connection.factories=org.apache.sqaop.teradata.TeradataManage rFactory'</pre> Si vous n'entrez aucun argument Sqoop, le service d'intégration de données construit la commande Sqoop en fonction des propriétés de connexion JDBC.

Options de connexion JDBC V2

Utilisez les options de connexion pour définir une connexion JDBC V2.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Par exemple :

```
./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-
appsdk.c5wj9sntucrg.ap-south-1.rds.amazonaws.com:5432/
JDBC_V2' jdbcdriverclassname='org.postgresql.Driver' schemaname='public'
subtype='PostgreSQL' supportmixedcaseidentifier='true'
quoteChar='(quotes) '"
```

Pour entrer plusieurs options, séparez-les par des espaces. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion JDBC V2 pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
username	Nom d'utilisateur de la base de données. Nom d'utilisateur avec autorisations d'accès à la base de données relationnelle, Azure SQL ou PostgreSQL.
password	Mot de passe du nom d'utilisateur de la base de données.
schemaname	Nom du schéma pour la connexion dans la base de données.
jdbcdriverclassname	Nom de classe du pilote JDBC. La liste suivante fournit le nom de classe du pilote que vous pouvez entrer pour le type de base de données concerné : <ul style="list-style-type: none">- Nom de classe du pilote JDBC pour Azure SQL Database : com.microsoft.sqlserver.jdbc.SQLServerDriver- Nom de classe du pilote JDBC pour Aurora PostgreSQL : org.postgresql.Driver Pour plus d'informations sur la classe de pilote à utiliser avec des bases de données spécifiques, consultez la documentation du fournisseur.
connectionstring	Chaîne de connexion permettant de se connecter à la base de données. Utilisez la chaîne de connexion suivante : jdbc:<subprotocol>:<subname> La liste suivante fournit des exemples de chaînes de connexion que vous pouvez entrer pour le type de base de données concerné : <ul style="list-style-type: none">- Chaîne de connexion pour le pilote JDBC d'Azure SQL Database : jdbc:informatica:oracle://<host>:<port>;SID=<value>- Chaîne de connexion pour le pilote JDBC d'Aurora PostgreSQL : jdbc:postgresql://<host>:<port>[/dbname] Pour plus d'informations sur la chaîne de connexion à utiliser avec des pilotes spécifiques, consultez la documentation du fournisseur.
subtype	Type de la base de données à laquelle vous souhaitez vous connecter. Vous pouvez sélectionner un des types de base de données suivants pour la connexion : <ul style="list-style-type: none">- Azure SQL Database. Connexion à Azure SQL Database.- PostgreSQL. Connexion à la base de données Aurora PostgreSQL.- Autres. Connexion à une base de données qui prend en charge le pilote JDBC de type 4.

Option	Description
supportmixedcaseidentifier	<p>Activez cette option si la base de données utilise des identificateurs sensibles à la casse. Lorsqu'il est activé, le service d'intégration de données entoure tous les identificateurs du caractère sélectionné pour la propriété Caractère identificateur SQL.</p> <p>Par exemple, la base de données PostgreSQL prend en charge les caractères de différentes casses. Vous devez activer cette propriété pour la connexion à la base de données PostgreSQL.</p> <p>Lorsque la propriété Caractère identificateur SQL est définie sur Aucun, la propriété Prise en charge des identificateurs à casse mixte est désactivée.</p>
quoteChar	<p>Type de caractère que la base de données utilise pour entourer des identificateurs délimités dans les requêtes SQL. Les caractères disponibles dépendent du type de la base de données.</p> <p>Sélectionnez (Aucun) si la base de données utilise des identificateurs classiques. Lorsque le service d'intégration de données génère des requêtes SQL, il ne place pas de caractères de délimitation autour des identificateurs.</p> <p>Sélectionnez un caractère si la base de données utilise des identificateurs délimités. Lorsque le service d'intégration de données génère des requêtes SQL, le service entoure les identificateurs délimités de ce caractère.</p>

Options de connexion JD Edwards EnterpriseOne

Utilisez les options de connexion pour définir une connexion JD Edwards EnterpriseOne.

Entrez les options de connexion au format suivant :

... -o option_name=value option_name=value ...

Par exemple :

```
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'
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion JD Edwards EnterpriseOne obligatoires pour les commandes infacmd isp CreateConnection et UpdateConnection :

Propriété	Description
userName	Nom d'utilisateur JD Edwards EnterpriseOne.
password	Mot de passe pour le nom d'utilisateur JD Edwards EnterpriseOne. Le mot de passe est sensible à la casse.
enterpriseServer	Nom d'hôte du serveur JD Edwards EnterpriseOne auquel vous voulez accéder.
enterprisePort	Numéro de port utilisé pour accéder au serveur JD Edwards EnterpriseOne.

Propriété	Description
environment	Nom de l'environnement JD Edwards EnterpriseOne auquel vous voulez vous connecter.
role	Rôle de l'utilisateur JD Edwards EnterpriseOne.

Options de connexion Kafka

Utilisez les options de connexion pour définir une connexion Kafka.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Kafka pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
connectionId	Chaîne utilisée par le service d'intégration de données pour identifier la connexion. L'ID n'est pas sensible à la casse. Il peut contenir jusqu'à 255 caractères et doit être unique dans le domaine. Vous ne pouvez pas modifier cette propriété après avoir créé la connexion. La valeur par défaut est le nom de la connexion.
connectionType	Requis. Le type de connexion est KAFKA.
name	Obligatoire. Le nom de la connexion. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Vous pouvez modifier cette propriété après avoir créé la connexion. Le nom ne peut pas dépasser 128 caractères, ni contenir des espaces ni les caractères spéciaux suivants : ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
connRetryTimeout	Nombre de secondes durant lequel le service d'intégration tente de se reconnecter au broker Kafka. Si la source ou la cible n'est pas disponible durant le délai que vous spécifiez, l'exécution du mappage s'arrête pour éviter toute perte de données.
kafkaBrokerVersion	Version du broker de messages Kafka. Vous pouvez entrer l'une des valeurs suivantes : - 0.10.1.x-2.0.0

Option	Description
kfkBrkList	<p>Combinaisons d'adresses IP et de ports de la liste de brokers du système de messagerie Kafka. Le format de la combinaison d'adresse IP et de port est le suivant :</p> <p><IP Address>:<port></p> <p>Vous pouvez entrer plusieurs combinaisons d'adresses IP et de ports séparées par des virgules.</p>
zkHostPortList	<p>Combinaison d'adresse IP et de port d'Apache ZooKeeper qui gère la configuration du broker de messages Kafka. Le format de la combinaison d'adresse IP et de port est le suivant :</p> <p><IP Address>:<port></p> <p>Vous pouvez entrer plusieurs combinaisons d'adresses IP et de ports séparées par des virgules.</p>

Options de connexion Kudu

Utilisez les options de connexion pour définir une connexion Kudu.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Kudu pour les commandes `infacmd isp CreateConnection` et `UpdateConnection` :

Propriété	Description
Nom	Le nom de la connexion. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Vous pouvez modifier cette propriété après avoir créé la connexion. Le nom ne peut pas dépasser 128 caractères ni contenir d'espaces ou les caractères spéciaux suivants : ~ ! \$ % ^ & * () - + = { } \ ; " ' < , > . ? /
ID	Chaîne utilisée par le service d'intégration de données pour identifier la connexion. L'ID n'est pas sensible à la casse. Il peut contenir jusqu'à 255 caractères et doit être unique dans le domaine. Vous ne pouvez pas modifier cette propriété après avoir créé la connexion. La valeur par défaut est le nom de la connexion.
Description	La description de la connexion. La description ne peut pas dépasser 4 000 caractères.
Emplacement	Domaine dans lequel vous voulez créer la connexion.
Type	Type de connexion. Sélectionnez Kudu.

Options de connexion LDAP

Utilisez les options de connexion pour définir une connexion LDAP.

Entrez les options de connexion au format suivant :

... -o option_name=value option_name=value ...

Par exemple :

```
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
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion LDAP obligatoires pour les commandes infacmd isp CreateConnection et UpdateConnection :

Propriété	Description
hostName	Nom d'hôte du serveur d'annuaire LDAP auquel vous souhaitez accéder.
port	Numéro de port utilisé pour accéder au serveur d'annuaire LDAP.
userName	Nom d'utilisateur LDAP.
password	Mot de passe pour le nom d'utilisateur LDAP. Le mot de passe est sensible à la casse.

Options de connexion LinkedIn

Utilisez les options de connexion pour définir une connexion LinkedIn.

Entrez les options de connexion au format suivant :

... -o option_name=value option_name=value ...

Pour entrer plusieurs options, séparez-les par un espace. Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion LinkedIn pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
ConsumerKey	La clé de l'API que vous obtenez lorsque vous créez l'application dans LinkedIn. LinkedIn utilise la clé pour identifier l'application.
ConsumerSecret	La clé secrète que vous obtenez lorsque vous créez l'application dans LinkedIn. LinkedIn utilise ce secret pour établir la propriété de la clé du client.
AccessToken	Jeton d'accès que l'utilitaire OAuth renvoie. L'application LinkedIn utilise ce jeton au lieu des justificatifs d'identité de l'utilisateur pour accéder aux ressources protégées.
AccessSecret	Le secret d'accès que l'utilitaire OAuth renvoie. Le secret établit la propriété du jeton.

Options de connexion MapR-DB

Utilisez les options de connexion pour définir une connexion HBase pour MapR-DB.

Entrez les options de connexion au format suivant :

... -o option_name=value option_name=value ...

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion HBase pour MapR-DB pour les commandes `infacmd isp CreateConnection` et `UpdateConnection` :

Option	Description
DATABASETYPE	Requis. Définissez la valeur sur <code>MapR-DB</code> et insérez-la entre guillemets simples.
clusterConfigId	ID de configuration de cluster associé au cluster Hadoop. Vous devez entrer un ID de configuration pour configurer une connexion HBase pour MapR-DB.
maprdbpath	<p>Requis. Définissez la valeur sur le chemin de la base de données qui contient la table MapR-DB à laquelle vous souhaitez vous connecter. Entrez un chemin d'accès de grappe MapR valide. Placez la valeur entre guillemets simples.</p> <p>Lorsque vous créez un objet de données HBase pour MapR-DB, vous pouvez parcourir uniquement les tables qui existent dans le chemin d'accès spécifié dans cette option. Vous ne pouvez pas accéder aux tables qui sont disponibles dans les sous-répertoires dans le chemin d'accès spécifié. Par exemple, si vous spécifiez <code>maprdbpath</code> en tant que <code>/user/Customers/</code>, vous pouvez accéder aux tables dans le répertoire <code>Customers</code>. Toutefois, si le répertoire <code>Customers</code> contient un sous-répertoire nommé <code>Regions</code>, vous ne pouvez pas accéder aux tables du répertoire suivant : <code>/utilisateur/clients/régions</code></p>

Options de connexion de stockage Blob Microsoft Azure

Utilisez les options de connexion pour définir une connexion de stockage Blob Microsoft Azure.

Entrez les options de connexion au format suivant :

... -o option_name=value option_name=value ...

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion de stockage Blob Microsoft Azure pour les commandes `infacmd isp CreateConnection` et `UpdateConnection` :

Option	Description
accountName	Nom du compte de stockage Blob Microsoft Azure.
authenticationtype	Type d'autorisation. Vous pouvez sélectionner l'un des mécanismes d'autorisation suivants : <ul style="list-style-type: none">- Autorisation par clé partagée- Signatures d'accès partagé
accountKey	Clé d'accès Microsoft Azure Blob Storage.

Option	Description
sharedaccesssignature	Signatures d'accès partagé. Remarque: Même si vous ne souhaitez pas utiliser l'autorisation d'accès partagé pour créer une connexion, définissez l'option dans la ligne de commande comme suit : sharedaccesssignature=' '
containerName	Conteneur racine ou sous-dossiers, avec leur chemin absolu.
endpointSuffix	Type de points de terminaison Microsoft Azure. Vous pouvez indiquer l'un des points de terminaison suivants : <ul style="list-style-type: none"> - core.windows.net : Par défaut - core.usgovcloudapi.net : Pour sélectionner les points de terminaison Microsoft Azure du gouvernement américain - core.chinacloudapi.cn : Inapplicable

Options de connexion Microsoft Azure Data Lake Storage Gen1

Utilisez les options de connexion pour définir une connexion Microsoft Azure Data Lake Storage Gen1.

Entrez les options de connexion au format suivant :

... -o option_name=value option_name=value ...

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Microsoft Azure Data Lake Storage Gen1 pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
ADLSAccountName	Nom du compte ou du service Microsoft Azure Data Lake Storage Gen1.
ClientId	ID de votre application utilisé pour terminer l'authentification OAuth dans Active Directory.
ClientSecret	Clé secrète client utilisée pour terminer l'authentification OAuth dans Active Directory.
Directory	Chemin d'un répertoire existant sous le système de fichiers donné. Le répertoire racine est le répertoire par défaut.
AuthEndpoint	Point de terminaison du jeton OAuth 2.0 à partir duquel le code d'accès est généré en fonction de l'ID de client et la clé secrète client est terminée.

Pour en savoir plus sur la création d'un ID client et d'une clé secrète client, contactez votre administrateur Azure ou consultez la documentation Microsoft Azure Data Lake Storage Gen1.

Options de connexion Microsoft Azure Data Lake Storage Gen2

Utilisez les options de connexion pour définir une connexion Microsoft Azure Data Lake Storage Gen2.

Entrez les options de connexion au format suivant :

... -o option_name=value option_name=value ...

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Microsoft Azure Data Lake Storage Gen2 pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
accountName	Nom du compte ou du service Microsoft Azure Data Lake Storage Gen2.
clientID	ID de votre application utilisé pour terminer l'authentification OAuth dans Active Directory.
clientSecret	Clé secrète client utilisée pour l'authentification OAuth dans Active Directory.
tenantID	ID de l'annuaire Azure Active Directory.
fileSystemName	Nom du système de fichiers existant dans Microsoft Azure Data Lake Storage Gen2.
directoryPath	Chemin d'un répertoire existant sous le système de fichiers donné. Le répertoire racine est le répertoire par défaut.

Pour en savoir plus sur la création d'un ID de client, d'une clé secrète client, d'un ID de locataire et d'un nom de système de fichiers, contactez votre administrateur Azure ou consultez la documentation Microsoft Azure Data Lake Storage Gen2.

Options de connexion Microsoft Azure SQL Data Warehouse

Utilisez les options de connexion pour définir une connexion Microsoft Azure SQL Data Warehouse.

Entrez les options de connexion au format suivant :

... -o option_name=value option_name=value ...

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Microsoft Azure SQL Data Warehouse pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
JdbcUrl	Chaîne de connexion JDBC Microsoft Azure SQL Data Warehouse. Par exemple, vous pouvez entrer la chaîne de connexion suivante : <code>jdbc:sqlserver://<Server>.database.windows.net:1433;database=<Database></code>
JdbcUsername	Nom d'utilisateur utilisé pour se connecter au compte Microsoft Azure SQL Data Warehouse.
JdbcPassword	Mot de passe utilisé pour se connecter au compte Microsoft Azure SQL Data Warehouse.
SchemaName	Nom du schéma dans Microsoft Azure SQL Data Warehouse.
BlobAccountName	Nom du compte du stockage Microsoft Azure utilisé pour le stockage intermédiaire des fichiers.
BlobAccountKey	Clé d'accès au stockage Microsoft Azure utilisée pour le stockage intermédiaire des fichiers.

Option	Description
EndPointSuffix	Type de points de terminaison Microsoft Azure. Vous pouvez indiquer l'un des points de terminaison suivants : <ul style="list-style-type: none"> - <code>core.windows.net</code> : Par défaut - <code>core.usgovcloudapi.net</code> : Pour sélectionner les points de terminaison Microsoft Azure du gouvernement américain - <code>core.chinacloudapi.cn</code> : Inapplicable
VNetRule	Activez cette option pour établir une connexion à un point de terminaison Microsoft Azure SQL Data Warehouse appartenant à un réseau virtuel (VNet).

Options de connexion Microsoft SQL Server

Utilisez les options de connexion pour définir la connexion Microsoft SQL Server.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Microsoft SQL Server pour les commandes `infacmd isp CreateConnection` et `UpdateConnection` :

Option	Description
UseTrustedConnection	Facultatif. Le service d'intégration utilise l'authentification Windows pour accéder à la base de données Microsoft SQL Server. Le nom d'utilisateur qui démarre le service d'intégration doit être celui d'un utilisateur Windows valide ayant accès à la base de données Microsoft SQL Server. True ou false. La valeur par défaut est False.
PassThruEnabled	Facultatif. Active la sécurité des intercommunications de la connexion. Lorsque vous activez la sécurité des intercommunications d'une connexion, le domaine utilise le nom d'utilisateur et le mot de passe du client au lieu des justificatifs d'identité définis dans l'objet de connexion pour se connecter à la base de données correspondante.

Option	Description
MetadataAccessConnectionString	<p>URL de connexion JDBC pour accéder aux métadonnées de la base de données. Utilisez l'URL de connexion suivante :</p> <pre>jdbc:informatica:sqlserver://<nom d'hôte>:<port>;DatabaseName=<nom de la base de données></pre> <p>Pour tester la connexion avec l'authentification NTLM, incluez les paramètres suivants dans la chaîne de connexion :</p> <ul style="list-style-type: none"> - AuthenticationMethod. Version de l'authentification NTLM à utiliser. <p>Remarque: UNIX prend en charge NTLMv1 et NTLMv2 mais pas NTLM.</p> <ul style="list-style-type: none"> - Domaine. Domaine auquel SQL Server appartient. <p>L'exemple suivant présente la chaîne de connexion pour un serveur SQL Server qui utilise l'authentification NTLMv2 dans un domaine NT Informatica.com :</p> <pre>jdbc:informatica:sqlserver://host01:1433;DatabaseName=SQL1;AuthenticationMethod=ntlm2java;Domain=Informatica.com</pre> <p>Si vous vous connectez à l'aide de l'authentification NTLM, vous pouvez activer l'option Utiliser une connexion approuvée dans les propriétés de connexion de MS SQL Server. Si vous vous connectez à l'aide de l'authentification NTLMv1 ou NTLMv2, vous devez fournir le nom d'utilisateur et le mot de passe dans les propriétés de connexion.</p>
AdvancedJDBCSecurityOptions	<p>Facultatif. Paramètres de base de données pour l'accès aux métadonnées d'une base de données sécurisée. Informatica traite la valeur du champ AdvancedJDBCSecurityOptions comme des données sensibles et crypte la chaîne de paramètres.</p> <p>Pour vous connecter à une base de données sécurisée, incluez les paramètres suivants :</p> <ul style="list-style-type: none"> - EncryptionMethod. Obligatoire. Indique si les données sont cryptées lorsqu'elles sont transmises sur le réseau. Ce paramètre doit être défini pour SSL. - ValidateServerCertificate. Facultatif. Indique si Informatica valide le certificat envoyé par le serveur de base de données. <p>Si ce paramètre est défini sur True, Informatica valide le certificat envoyé par le serveur de base de données. Si vous spécifiez le paramètre HostNameInCertificate, Informatica valide également le nom d'hôte dans le certificat.</p> <p>Si ce paramètre est défini sur false, Informatica ne valide pas le certificat envoyé par le serveur de base de données. Informatica ignore les informations de truststore que vous spécifiez.</p> <ul style="list-style-type: none"> - HostNameInCertificate. Facultatif. Nom d'hôte de la machine qui héberge la base de données sécurisée. Si vous spécifiez un nom d'hôte, Informatica valide le nom d'hôte inclus dans la chaîne de connexion avec le nom d'hôte dans le certificat SSL. - TrustStore. Obligatoire. Chemin et nom du fichier truststore contenant le certificat SSL de la base de données. - TrustStorePassword. Obligatoire. Mot de passe du fichier truststore de la base de données sécurisée. <p>Remarque: Pour obtenir la liste complète des paramètres JDBC sécurisés, consultez la documentation de DataDirect JDBC.</p> <p>Informatica ajoute les paramètres JDBC sécurisés à la chaîne de connexion. Si vous incluez les paramètres JDBC sécurisés directement dans la chaîne de connexion, n'entrez aucun paramètre dans le champ AdvancedJDBCSecurityOptions.</p>
DataAccessConnectionString	<p>Obligatoire. Chaîne de connexion utilisée pour accéder aux données de la base de données.</p> <p>Entrez la chaîne de connexion au format suivant :</p> <pre><nom du serveur>@<nom de la base de données></pre>

Option	Description
DomainName	Facultatif. Nom du domaine dans lequel Microsoft SQL Server est exécuté.
PacketSize	Facultatif. Augmentez la taille des paquets réseau pour permettre à des paquets des données plus importants de transiter par le réseau à un moment donné.
CodePage	Obligatoire. Code devant être lu dans la base de données ou écrit dans celle-ci. Utilisez le nom de la page du code ISO, par exemple ISO-8859-6. Le nom de la page du code n'est pas sensible à la casse.
UseDSN	Obligatoire. Détermine si le service d'intégration de données doit utiliser le nom de la source de données pour la connexion. Si vous définissez la valeur sur True, le service d'intégration de données récupère le nom de la base de données et le nom de serveur à partir du DSN. Si vous définissez la valeur sur False, vous devez entrer le nom de la base de données et le nom du serveur.
ProviderType	Obligatoire. Fournisseur de connexion que vous souhaitez utiliser pour vous connecter à la base de données Microsoft SQL Server. Vous pouvez définir l'une des valeurs suivantes : <ul style="list-style-type: none"> - 0. Définissez la valeur sur 0 si vous souhaitez utiliser le fournisseur ODBC. La valeur par défaut est 0. - 1. Définissez la valeur sur 1 si vous souhaitez utiliser le fournisseur OLEDB.
OwnerName	Facultatif. Nom du propriétaire de la table.
SchemaName	Facultatif. Nom du schéma dans la base de données. Vous devez indiquer le nom du schéma de l'entrepôt de profilage s'il est différent du nom d'utilisateur de la base de données. Vous devez spécifier le nom du schéma pour la base de données du cache d'objet de données s'il diffère du nom d'utilisateur de base de données et si vous configurez des tables de cache gérées par l'utilisateur.
EnvironmentSQL	Facultatif. Commandes SQL permettant de définir l'environnement de base de données lorsque vous vous connectez à la base de données. Le service d'intégration de données exécute le SQL de l'environnement de connexion à chaque connexion à la base de données. Par exemple, <code>ALTER SESSION SET CURRENT_SCHEMA=INFA_USR;</code> Remarque: Placez les caractères spéciaux entre guillemets doubles.
TransactionSQL	Facultatif. Commandes SQL à exécuter avant chaque transaction. Le service d'intégration de données exécute le SQL transactionnel au début de chaque transaction. Par exemple, <code>SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;</code> Remarque: Placez les caractères spéciaux entre guillemets doubles.
QuoteChar	Facultatif. Caractère que vous utiliserez pour les guillemets dans cette connexion. Type de caractère servant à identifier les caractères spéciaux et les mots clés SQL réservés, tels que WHERE. Le service d'intégration de données place le caractère sélectionné autour des caractères spéciaux et des mots clés SQL réservés. Le service d'intégration de données utilise également ce caractère pour la propriété QuoteChar. La valeur par défaut est 0.

Option	Description
EnableQuotes	Facultatif. Choisissez cette option pour activer les guillemets pour cette connexion. Lorsque cette option est activée, le service d'intégration de données place les caractères identifiants autour des noms de table, de vue, de schéma, de synonyme et de colonne lors de la génération et de l'exécution de SQL par rapport à ces objets dans la connexion. Utilisez-la si les objets comportent une casse mixte ou des noms en minuscules. Les valeurs valides sont True ou False. La valeur par défaut est True.
EnableConnectionPool	Facultatif. Active le pooling de connexions. Lorsque vous activez le pooling de connexions, celui-ci conserve les instances de connexion inactives en mémoire. Lorsque vous désactivez le pooling de connexions, le service d'intégration de données arrête toute l'activité du pooling. Les valeurs valides sont True ou False. La valeur par défaut est True.
ConnectionPoolSize	Facultatif. Nombre maximal d'instances de connexion inactives que le service d'intégration de données gère pour une connexion de base de données. Définissez cette valeur à une valeur supérieure au nombre minimal d'instances de connexion inactives. La valeur par défaut est 15.
ConnectionPoolMaxIdleTime	Facultatif. Nombre de secondes pendant lesquelles une connexion qui dépasse le nombre minimal d'instances de connexion peut rester inactive avant que le pool de connexions ne l'abandonne. Le pool de connexions ignore la durée d'inactivité lorsque celle-ci ne dépasse pas le nombre minimal d'instances de connexion inactives. La valeur par défaut est 120.
ConnectionPoolMinConnections	Facultatif. Nombre minimal d'instances de connexion inactives que le pool maintient pour une connexion de base de données. Définissez cette valeur comme étant égale ou inférieure à la taille du pool de connexions inactives. La valeur par défaut est 0.

Options de connexion Microsoft Dynamics CRM

Utilisez les options de connexion pour définir une connexion Microsoft Dynamics CRM.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Par exemple :

```
./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>"
```

Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Microsoft Dynamics CRM pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
AuthenticationType	<p>Requis. Type d'authentification pour la connexion. Fournissez l'un des types d'authentification suivants :</p> <ul style="list-style-type: none"> - Passport. Souvent utilisé pour le déploiement en ligne et le déploiement en ligne combiné avec le déploiement avec accès via Internet de Microsoft Dynamics CRM. - Basé sur les revendications. Souvent utilisé pour le déploiement local et le déploiement avec accès via Internet de Microsoft Dynamics CRM. - Active Directory. Souvent utilisé pour le déploiement local de Microsoft Dynamics CRM.
DiscoveryServiceURL	<p>Requis. URL du service Microsoft Dynamics CRM.</p> <p>Utilisez le format suivant : <http/https>://<Application server name> :<port>/XRMServices/2011/Discovery.svc</p> <p>Pour rechercher l'URL du service de découverte, connectez-vous à l'instance Microsoft Live et cliquez sur Settings > Customization > Developer Resources.</p>
Domaine	<p>Requis. Domaine auquel appartient l'utilisateur. Vous devez fournir le nom de domaine complet. Par exemple, msd.sampledomain.com.</p> <p>Configurez le domaine pour l'authentification Active Directory et basée sur les revendications.</p> <p>Remarque: Si vous sélectionnez le type d'authentification Passport, vous devez fournir une valeur factice pour le domaine.</p>
ConfigFilesForMetadata	<p>Répertoire de configuration du client.</p> <p>Le répertoire par défaut est : <INFA_HOME>/clients/DeveloperClient/msdcrm/conf</p>
OrganizationName	<p>Requis. Nom de l'organisation Microsoft Dynamics CRM. Les noms d'organisation sont sensibles à la casse.</p> <p>Pour l'authentification Microsoft Live, utilisez le nom unique de l'organisation Microsoft Live.</p> <p>Pour trouver le nom unique de l'organisation, connectez-vous à l'instance Microsoft Live et cliquez sur Settings > Customization > Developer Resources</p>
Mot de passe	Requis. Mot de passe utilisé pour authentifier l'utilisateur.
ConfigFilesForData	<p>Répertoire de configuration du serveur.</p> <p>Si le fichier du serveur se trouve dans un répertoire différent, spécifiez le chemin d'accès au répertoire.</p>
SecurityTokenService	<p>Requis. URL du service de jeton de sécurité Microsoft Dynamics CRM. Par exemple, https://sts1.<company>.com.</p> <p>Configurez pour l'authentification basée sur les revendications.</p> <p>Remarque: Si vous sélectionnez le type d'authentification Passport ou Active Directory, vous devez fournir une valeur factice pour SecurityTokenService.</p>
Nom d'utilisateur	Requis. ID utilisateur enregistré avec Microsoft Dynamics CRM.

Option	Description
UseMetadataConfigForDataAccess	Sélectionnez cette option si le fichier de configuration et le fichier du serveur se trouvent dans le même répertoire. Si le fichier du serveur se trouve dans un autre répertoire, désélectionnez cette option et spécifiez le chemin d'accès au répertoire dans le champ Accès aux données. Fournissez l'une des valeurs suivantes : - true pour sélectionnée - false pour désélectionnée
KeyStoreFileName	Contient les clés et certificats requis pour une communication sécurisée. Si vous souhaitez utiliser le fichier Java cacerts, désélectionnez ce champ.
KeyStorePassword	Mot de passe du fichier <code>infa_keystore.jks</code> . Si vous souhaitez utiliser le fichier Java cacerts, désélectionnez ce champ.
TrustStoreFileName	Définissez INFA_TRUSTSTORE dans les variables d'environnement. Le répertoire doit contenir le fichier truststore <code>infa_truststore.jks</code> . Si le fichier n'est pas disponible sur le chemin d'accès spécifié, le service d'intégration de données vérifie le certificat dans le fichier Java cacerts. Si vous souhaitez utiliser le fichier Java cacerts, désélectionnez ce champ.
TrustStorePassword	Mot de passe du fichier <code>infa_keystore.jks</code> . Si vous souhaitez utiliser le fichier Java cacerts, désélectionnez ce champ.

Options de connexion Netezza

Utilisez les options de connexion pour définir une connexion Netezza.

Entrez les options de connexion au format suivant :

... -o option_name=value option_name=value ...

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Netezza pour les commandes `infacmd isp` `CreateConnection` et `UpdateConnection` :

Option	Description
connectionString	Requis. Nom de la source de données ODBC que vous créez pour vous connecter à la base de données Netezza.
jdbcUrl	Requis. URL JDBC que l'outil Developer tool doit utiliser lorsqu'il se connecte à la base de données Netezza. Utilisez le format suivant : <code>jdbc:netezza://<hostname>:<port>/<database name></code>
nom d'utilisateur	Requis. Nom d'utilisateur disposant des autorisations appropriées pour accéder à la base de données Netezza.
mot de passe	Requis. Mot de passe pour le nom d'utilisateur de la base de données.
délai d'expiration	Requis. Nombre de secondes pendant lesquelles l'outil Developer tool attend une réponse de la base de données Netezza avant de fermer la connexion.

Options de connexion OData

Utilisez les options de connexion pour définir une connexion OData.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion OData pour les commandes `infacmd isp CreateConnection` et `UpdateConnection` :

Propriété	Description
URL	Requis. URL de racine de service OData qui présente les données que vous voulez lire.
securityType	Facultatif. Protocole de sécurité que l'outil Developer tool doit utiliser pour établir une connexion sécurisée avec le serveur OData. Entrez l'une des valeurs suivantes : <ul style="list-style-type: none">- Aucun- SSL- TLS
trustStoreFileName	Requis si vous sélectionnez un type de sécurité. Nom du fichier truststore contenant le certificat public du serveur OData.
trustStorePassword	Requis si vous sélectionnez un type de sécurité. Mot de passe du fichier truststore contenant le certificat public du serveur OData.
keyStoreFileName	Requis si vous sélectionnez un type de sécurité. Nom du fichier keystore qui contient la clé privée du serveur OData.
keyStorePassword	Requis si vous sélectionnez un type de sécurité. Mot de passe du fichier keystore qui contient la clé privée du serveur OData.

Options de connexion ODBC

Utilisez les options de connexion pour définir une connexion ODBC.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion ODBC pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
PassThruEnabled	Facultatif. Active la sécurité des intercommunications de la connexion. Lorsque vous activez la sécurité des intercommunications d'une connexion, le domaine utilise le nom d'utilisateur et le mot de passe du client au lieu des justificatifs d'identité définis dans l'objet de connexion pour se connecter à la base de données correspondante.
DataAccessConnectionString	Chaîne de connexion utilisée pour accéder aux données de la base de données. Entrez la chaîne de connexion au format suivant : <nom de la base de données>
CodePage	Obligatoire. Page de code utilisée pour lire une base de donnée source ou écrire dans une base de données ou un fichier cibles.
EnvironmentSQL	Facultatif. Commandes SQL permettant de définir l'environnement de base de données lorsque vous vous connectez à la base de données. Le service d'intégration de données exécute le SQL de l'environnement de connexion à chaque connexion à la base de données. Par exemple, <code>ALTER SESSION SET CURRENT_SCHEMA=INFA_USR;</code> Remarque: Placez les caractères spéciaux entre guillemets doubles.
TransactionSQL	Facultatif. Commandes SQL à exécuter avant chaque transaction. Le service d'intégration de données exécute le SQL transactionnel au début de chaque transaction. Par exemple, <code>SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;</code> Remarque: Placez les caractères spéciaux entre guillemets doubles.
QuoteChar	Facultatif. Caractère que vous utiliserez pour les guillemets dans cette connexion. Type de caractère servant à identifier les caractères spéciaux et les mots clés SQL réservés, tels que WHERE. Le service d'intégration de données place le caractère sélectionné autour des caractères spéciaux et des mots clés SQL réservés. Le service d'intégration de données utilise également ce caractère pour la propriété QuoteChar. La valeur par défaut est 4.
Fournisseur ODBC	Facultatif. Type de base de données auquel le service d'intégration de données se connecte via ODBC. Pour une optimisation du refoulement, indiquez le type de base de données afin que le service d'intégration de données génère une base de données SQL native. Les options sont les suivantes : <ul style="list-style-type: none"> - Autre - Sybase - Microsoft_SQL_Server - Teradata - Netezza - Greenplum La valeur par défaut est Autre.

Option	Description
EnableQuotes	Facultatif. Choisissez cette option pour activer les guillemets pour cette connexion. Lorsque cette option est activée, le service d'intégration de données place les caractères identifiants autour des noms de table, de vue, de schéma, de synonyme et de colonne lors de la génération et de l'exécution de SQL par rapport à ces objets dans la connexion. Utilisez-la si les objets comportent une casse mixte ou des noms en minuscules. Les valeurs valides sont True ou False. La valeur par défaut est False.
EnableConnectionPool	Facultatif. Active le pooling de connexions. Lorsque vous activez le pooling de connexions, le pool de connexions conserve les instances de connexion inactives en mémoire. Lorsque vous désactivez le pooling de connexions, le service d'intégration de données arrête toutes les activités de pooling. Les valeurs valides sont True ou False. La valeur par défaut est True.
ConnectionPoolSize	Facultatif. Nombre maximum d'instances de connexion inactives que le service d'intégration de données gère pour une connexion de base de données. Définissez cette valeur à une valeur supérieure au nombre minimum d'instances de connexion inactives. La valeur par défaut est 15.
ConnectionPoolMaxIdleTime	Facultatif. Nombre de secondes qu'une connexion qui dépasse le nombre minimum d'instances de connexion peut rester inactive avant que le pool de connexions ne l'abandonne. Le pool de connexions ignore la durée d'inactivité lorsque celle-ci ne dépasse pas le nombre minimum d'instances de connexion inactives. Par défaut 120.
ConnectionPoolMinConnections	Facultatif. Le nombre minimum d'instances de connexion inactives que le pool maintient pour une connexion de base de données. Définissez cette valeur à une valeur égale ou inférieure à la taille du pool de connexions inactives. La valeur par défaut est 0.

Options de connexion Oracle

Utilisez les options de connexion pour définir une connexion Oracle.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Oracle pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
PassThruEnabled	Facultatif. Active la sécurité des intercommunications de la connexion. Lorsque vous activez la sécurité des intercommunications d'une connexion, le domaine utilise le nom d'utilisateur et le mot de passe du client au lieu des justificatifs d'identité définis dans l'objet de connexion pour se connecter à la base de données correspondante.
MetadataAccessConnectionString	URL de connexion JDBC utilisée pour accéder aux métadonnées de la base de données. jdbc:informatica:oracle://<nom de l'hôte>:<port>;SID=<nom de la base de données>
AdvancedJDBCSecurityOptions	<p>Facultatif. Paramètres de base de données pour l'accès aux métadonnées d'une base de données sécurisée. Informatica traite la valeur du champ AdvancedJDBCSecurityOptions comme des données sensibles et crypte la chaîne de paramètres.</p> <p>Pour vous connecter à une base de données sécurisée, incluez les paramètres suivants :</p> <ul style="list-style-type: none"> - EncryptionMethod. Requis. Indique si les données sont cryptées lorsqu'elles sont transmises sur le réseau. Ce paramètre doit être défini pour SSL. - ValidateServerCertificate. Facultatif. Indique si Informatica valide le certificat envoyé par le serveur de base de données. <p>Si ce paramètre est défini sur True, Informatica valide le certificat envoyé par le serveur de base de données. Si vous spécifiez le paramètre HostNameInCertificate, Informatica valide également le nom d'hôte dans le certificat.</p> <p>Si ce paramètre est défini sur false, Informatica ne valide pas le certificat envoyé par le serveur de base de données. Informatica ignore les informations de truststore que vous spécifiez.</p> <ul style="list-style-type: none"> - HostNameInCertificate. Facultatif. Nom d'hôte de la machine qui héberge la base de données sécurisée. Si vous spécifiez un nom d'hôte, Informatica valide le nom d'hôte inclus dans la chaîne de connexion avec le nom d'hôte dans le certificat SSL. - TrustStore. Requis. Chemin et nom du fichier truststore contenant le certificat SSL de la base de données. - TrustStorePassword. Requis. Mot de passe du fichier truststore de la base de données sécurisée. - Keystore. Requis. Chemin d'accès et nom du fichier keystore. - Mot de passe keystore. Mot de passe du fichier keystore de la base de données sécurisée. <p>Remarque: Pour obtenir la liste complète des paramètres JDBC sécurisés, consultez la documentation de DataDirect JDBC.</p> <p>Informatica ajoute les paramètres JDBC sécurisés à la chaîne de connexion. Si vous incluez les paramètres JDBC sécurisés directement dans la chaîne de connexion, n'entrez aucun paramètre dans le champ AdvancedJDBCSecurityOptions.</p>
DataAccessConnectionString	Chaîne de connexion utilisée pour accéder aux données de la base de données. Entrez la chaîne de connexion au format suivant dans l'entrée TNSNAMES : <nom de la base de données>

Option	Description
CodePage	Requis. Page de code utilisée pour la lecture depuis une base de données source ou pour l'écriture dans une base de données ou un fichier cible.
EnvironmentSQL	Facultatif. Commandes SQL permettant de définir l'environnement de base de données lorsque vous vous connectez à la base de données. Le service d'intégration de données exécute le SQL de l'environnement de connexion à chaque connexion à la base de données. Par exemple, <code>ALTER SESSION SET CURRENT_SCHEMA=INFA_USR;</code> Remarque: Placez les caractères spéciaux entre guillemets doubles.
TransactionSQL	Facultatif. Commandes SQL à exécuter avant chaque transaction. Le service d'intégration de données exécute le SQL transactionnel au début de chaque transaction. Par exemple, <code>SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;</code> Remarque: Placez les caractères spéciaux entre guillemets doubles.
EnableParallelMode	Facultatif. Active le traitement parallèle lors du chargement des données dans une table en mode groupé. Utilisé pour Oracle. True ou false. La valeur par défaut est False.
QuoteChar	Facultatif. Caractère que vous utiliserez pour les guillemets dans cette connexion. Type de caractère servant à identifier les caractères spéciaux et les mots clés SQL réservés, tels que WHERE. Le service d'intégration de données place le caractère sélectionné autour des caractères spéciaux et des mots clés SQL réservés. Le service d'intégration de données utilise également ce caractère pour la propriété QuoteChar. La valeur par défaut est 0.
EnableQuotes	Facultatif. Choisissez cette option pour activer les guillemets pour cette connexion. Lorsque cette option est activée, le service d'intégration de données place les caractères identifiants autour des noms de table, de vue, de schéma, de synonyme et de colonne lors de la génération et de l'exécution de SQL par rapport à ces objets dans la connexion. Utilisez-la si les objets comportent une casse mixte ou des noms en minuscules. Les valeurs valides sont True ou False. La valeur par défaut est True.
EnableConnectionPool	Facultatif. Active le pooling de connexions. Lorsque vous activez le pooling de connexions, celui-ci conserve les instances de connexion inactives en mémoire. Lorsque vous désactivez le pooling de connexions, le service d'intégration de données arrête toute l'activité du pooling. Les valeurs valides sont True ou False. La valeur par défaut est True.
ConnectionPoolSize	Facultatif. Nombre maximal d'instances de connexion inactives que le service d'intégration de données gère pour une connexion de base de données. Définissez cette valeur à une valeur supérieure au nombre minimal d'instances de connexion inactives. La valeur par défaut est 15.

Option	Description
ConnectionPoolMaxIdleTime	Facultatif. Nombre de secondes pendant lesquelles une connexion qui dépasse le nombre minimal d'instances de connexion peut rester inactive avant que le pool de connexions ne l'abandonne. Le pool de connexions ignore la durée d'inactivité lorsque celle-ci ne dépasse pas le nombre minimal d'instances de connexion inactives. La valeur par défaut est 120.
ConnectionPoolMinConnections	Facultatif. Nombre minimal d'instances de connexion inactives que le pool maintient pour une connexion de base de données. Définissez cette valeur comme étant égale ou inférieure à la taille du pool de connexions inactives. La valeur par défaut est 0.

Options de connexion Salesforce

Utilisez les options de connexion pour définir une connexion Salesforce.

Entrez les options de connexion au format suivant :

... -o option_name=value option_name=value ...

Exemple de connexion Salesforce utilisant `infacmd`

```
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
```

Exemple de connexion Salesforce OAuth utilisant `pmcmd`

```
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
```

Exemple de connexion Salesforce standard utilisant `pmcmd`

```
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
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Salesforce pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
Nom d'utilisateur	Nom d'utilisateur Salesforce.
Mot de passe	Mot de passe correspondant au nom d'utilisateur Salesforce. Le mot de passe est sensible à la casse. Pour accéder à Salesforce en dehors du réseau approuvé de votre organisation, vous devez ajouter un jeton de sécurité à votre mot de passe pour vous connecter à l'API ou à un client de bureau. Pour recevoir ou réinitialiser votre jeton de sécurité, connectez-vous à Salesforce et cliquez sur Configuration > Mes informations personnelles > Réinitialiser mon jeton de sécurité .
Jeton d'actualisation	Pour la connexion Salesforce OAuth. Jeton d'actualisation de Salesforce généré à l'aide de la clé du consommateur et du secret du consommateur.
Clé du consommateur	Pour la connexion Salesforce OAuth. Clé du consommateur obtenue à partir de Salesforce, requise pour générer le jeton d'actualisation. Pour plus d'informations sur la génération de la clé du consommateur, consultez la documentation de Salesforce.
Secret du consommateur	Pour la connexion Salesforce OAuth. Secret du consommateur obtenu à partir de Salesforce, requis pour générer le jeton d'actualisation. Pour plus d'informations sur la génération du secret du consommateur, consultez la documentation de Salesforce.
Type de connexion	Sélectionnez la connexion Salesforce standard ou OAuth.
URL du service	URL du service Salesforce auquel vous voulez accéder. Dans un environnement de test ou de développement, il se peut que vous souhaitiez accéder à l'environnement de test Salesforce Sandbox. Pour plus d'informations sur Salesforce Sandbox, consultez la documentation Salesforce.

Options de connexion Salesforce Marketing Cloud

Utilisez les options de connexion pour définir une connexion Salesforce Marketing Cloud.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Exemple de commande 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
```

Exemple de commande 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
```

Exemple de commande infacmd removeConnection :

```
./infacmd.sh removeConnection -dn DomainName -un Domain_UserName -pd Domain_Pwd -cn
Connection_Name
```

Le tableau suivant décrit les options de connexion Salesforce Marketing Cloud pour les commandes infacmd.sh createConnection, updateConnection et remove :

Propriété de connexion	Description
Nom du domaine	Domaine Informatica dans lequel vous voulez créer la connexion.
Nom d'utilisateur du domaine	Nom d'utilisateur du domaine.
Mot de passe du domaine	Mot de passe du domaine.
Nom de la connexion	Nom de la connexion Salesforce Marketing Cloud.
ID de connexion	Le service d'intégration de données utilise l'ID pour identifier la connexion.
URL de Salesforce Marketing Cloud	<p>URL que le service d'intégration de données utilise pour établir la connexion WSDL à Salesforce Marketing Cloud.</p> <p>Exemple d'URL pour OAuth 1.0 :</p> <p><code>https://webservice.s7.exacttarget.com/etframework.wsdl</code></p> <p>Exemple d'URL pour OAuth 2.0 :</p> <p><code>https://<SUBDOMAIN>.soap.marketingcloudapis.com/etframework.wsdl</code></p> <p>Informatica recommande d'effectuer la mise à niveau vers OAuth 2.0 avant que Salesforce Marketing Cloud n'arrête la prise en charge d'OAuth 1.0.</p>
Nom d'utilisateur	Nom d'utilisateur du compte Salesforce Marketing Cloud.
Mot de passe	Mot de passe du compte Salesforce Marketing Cloud.
ClientId	ID du client Salesforce Marketing Cloud requis pour générer un jeton d'accès valide.
ClientSecret	Clé secrète du client Salesforce Marketing Cloud requise pour générer un jeton d'accès valide.
Activer la journalisation	Lorsque vous activez la journalisation, vous pouvez afficher le journal de session pour les tâches.
Décalage UTC	L'agent sécurisé utilise la propriété de connexion de décalage UTC à partir de laquelle lire et enregistrer des données dans Salesforce Marketing Cloud dans le fuseau horaire de décalage UTC.
Taille du lot	<p>Nombre de lignes que l'agent sécurisé enregistre dans un lot vers la cible.</p> <p>Lorsque vous insérez ou mettez à jour des données et spécifiez la clé de contact, les données associées à l'ID de contact spécifié sont insérées ou mises à jour dans un lot vers Salesforce Marketing Cloud. Lorsque vous effectuez un upsert des données dans Salesforce Marketing Cloud, ne spécifiez pas de clé de contact.</p>

Options de connexion SAPAPPLICATIONS

Utilisez les options de connexion pour définir la connexion SAPAPPLICATIONS.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion SAPAPPLICATIONS pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
UserName	Requis. Nom d'utilisateur système SAP.
Mot de passe	Requis. Mot de passe pour le nom d'utilisateur.
HostName	Obligatoire. Nom d'hôte de l'application SAP.
ClientNumber	Requis. Numéro du client SAP.
SystemNumber	Obligatoire. Numéro du système SAP.
Langue	Facultatif. Langue de connexion SAP.

Options de connexion séquentielle

Utilisez les options de connexion SEQ pour définir une connexion à un ensemble de données séquentielles z/OS.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion SEQ pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
CodePage	Requis. Code pour lire ou écrire dans le fichier séquentiel. Utilisez le nom de la page du code ISO, par exemple ISO-8859-6. Le nom de la page du code n'est pas sensible à la casse.
ArraySize	Facultatif. Détermine le nombre d'enregistrements dans la matrice de stockage pour les threads lorsque la valeur des threads de travail est supérieure à 0. Les valeurs valides sont comprises entre 1 et 5 000. La valeur par défaut est 25.
Compression	Facultatif. Comprime les données pour réduire le volume de données que les applications Informatica écrivent sur le réseau. True ou false. La valeur par défaut est False.

Option	Description
EncryptionLevel	<p>Facultatif. Niveau de chiffrement. Si vous spécifiez AES pour l'option EncryptionType, spécifiez l'une des valeurs suivantes pour indiquer le niveau de chiffrement AES :</p> <ul style="list-style-type: none"> - 1. Utilisez une clé de chiffrement 128 bits. - 2. Utilisez une clé de chiffrement 192 bits. - 3. Utilisez une clé de chiffrement 256 bits. <p>La valeur par défaut est 1.</p> <p>Remarque: Si vous sélectionnez Aucun pour le type de chiffrement, le service d'intégration de données ignore la valeur de niveau de chiffrement.</p>
EncryptionType	<p>Facultatif. Entrez l'une des valeurs suivantes pour le type de cryptage :</p> <ul style="list-style-type: none"> - Aucun - AES <p>La valeur par défaut est Aucun.</p> <p>Facultatif. Vérifie s'il faut utiliser le chiffrement. Spécifiez l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> - Aucun - AES <p>La valeur par défaut est Aucun.</p>
InterpretAsRows	<p>Facultatif. Si la valeur est « Vrai », la taille de stimulation représente un nombre de lignes. Si la valeur est False, la taille de stimulation représente des kilooctets. La valeur par défaut est False.</p>
Emplacement	<p>Emplacement du nœud de l'Écouteur PowerExchange qui peut se connecter à la source de données. L'emplacement est défini dans le premier paramètre de l'instruction NODE dans le fichier de configuration dbmover.cfg de PowerExchange.</p>
OffLoadProcessing	<p>Facultatif. Déplace le traitement des données en bloc depuis la machine source de données à la machine du service d'intégration de données.</p> <p>Entrez l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> - Auto. Le service d'intégration de données détermine si vous souhaitez utiliser le traitement de déchargement. - Oui. Utiliser le traitement de déchargement. - Non. Ne pas utiliser le traitement de déchargement. <p>La valeur par défaut est Auto.</p>
PacingSize	<p>Facultatif. Ralentit le taux de transfert de données pour réduire les goulets d'étranglement. Plus la valeur est basse, plus les performances de la session sont élevées. La valeur minimale est 0. Entrez 0 pour des performances optimales. La valeur par défaut est 0.</p>
WorkerThread	<p>Facultatif. Nombre de threads que le service d'intégration de données utilise pour traiter les données en bloc lorsque le traitement du déchargement est activé. Pour des performances optimales, cette valeur ne doit pas dépasser le nombre de processeurs disponibles sur la machine du service d'intégration de données. Les valeurs valides vont de 1 à 64. La valeur par défaut est 0, ce qui désactive le multithreading.</p>
WriteMode	<p>Entrez l'un des modes d'écriture suivants :</p> <ul style="list-style-type: none"> - CONFIRMWRITEON. Envoie des données au service d'intégration de données et attend la réponse de réussite/échec avant d'envoyer davantage de données. - CONFIRMWRITEOFF. Envoie des données au service d'intégration de données sans attendre la réponse de réussite/échec. Utilisez cette option lorsque la table cible peut être rechargée si une erreur se produit. - ASYNCHRONOUSWITHFAULTT. Envoie des données au service d'intégration de données de manière asynchrone avec la possibilité de détecter les erreurs. <p>La valeur par défaut est CONFIRMWRITEON.</p>

Option	Description
EnableConnectionPool	Facultatif. Active le pooling de connexions. Lorsque vous activez le pooling de connexions, celui-ci conserve les instances de connexion inactives en mémoire. Lorsque vous désactivez le pooling de connexions, le service d'intégration de données arrête toute l'activité du pooling. True ou false. La valeur par défaut est False.
ConnectionPoolSize	Facultatif. Nombre maximal d'instances de connexion inactives que le service d'intégration de données gère pour une connexion de base de données. Définissez cette valeur à une valeur supérieure au nombre minimal d'instances de connexion inactives. La valeur par défaut est 15.
ConnectionPoolMaxIdle Time	Facultatif. Nombre de secondes pendant lesquelles une connexion qui dépasse le nombre minimal d'instances de connexion peut rester inactive avant que le pool de connexions ne l'abandonne. Le pool de connexions ignore la durée d'inactivité lorsque celle-ci ne dépasse pas le nombre minimal d'instances de connexion inactives. La valeur par défaut est 120.
ConnectionPoolMinConnections	Facultatif. Nombre minimal d'instances de connexion inactives que le pool maintient pour une connexion de base de données. Définissez cette valeur comme étant égale ou inférieure à la taille du pool de connexions inactives. La valeur par défaut est 0.

Options de connexion Snowflake

Utilisez les options de connexion pour définir une connexion Snowflake.

Entrez les options de connexion au format suivant :

... -o option_name=value option_name=value ...

Par exemple :

```
./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"
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Snowflake obligatoires pour les commandes infacmd isp CreateConnection et UpdateConnection :

Propriété	Description
connectionId	Chaîne utilisée par le service d'intégration de données pour identifier la connexion.
connectionType	Type de connexion. Le type de connexion est Snowflake.
name	Nom de la connexion.
account	Nom du compte Snowflake.
additionalparam	Entrez au moins un paramètre de connexion JDBC au format suivant : <param1>=<value>&<param2>=<value>&<param3>=<value>... Par exemple : user=jon&warehouse=mywh&db=mydb&schema=public

Propriété	Description
password	Mot de passe pour la connexion au compte Snowflake.
role	Rôle Snowflake attribué à l'utilisateur.
user	Nom d'utilisateur pour la connexion au compte Snowflake.
warehouse	Nom de l'entrepôt Snowflake.

Options de connexion Tableau

Utilisez les options de connexion pour définir une connexion Tableau.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Par exemple :

```
./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"
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Tableau obligatoires pour les commandes infacmd isp CreateConnection et UpdateConnection :

Propriété de connexion	Description
Produit Tableau	Nom du produit Tableau auquel vous souhaitez vous connecter. Vous pouvez choisir l'un des produits Tableau suivants pour publier le fichier TDE ou TWBX : - Tableau Desktop. Crée un fichier TDE sur la machine du service d'intégration de données. Vous pouvez ensuite importer manuellement le fichier TDE dans Tableau Desktop. - Tableau Server Publie le fichier TDE ou TWBX généré sur Tableau Server. - Tableau Online. Publie le fichier TDE ou TWBX généré sur Tableau Online.
URL de connexion	URL du produit Tableau Server ou Tableau Online sur lequel vous souhaitez publier le fichier TDE ou TWBX. L'URL a le format suivant : <code>http://<nom d'hôte de Tableau Server ou Tableau Online>:<port></code>
Nom d'utilisateur	Nom d'utilisateur du compte Tableau Server ou Tableau Online.
Mot de passe	Mot de passe du compte Tableau Server ou Tableau Online.
URL du contenu	Nom du site sur Tableau Server ou Tableau Online où vous souhaitez publier le fichier TDE ou TWBX. Contactez l'administrateur de Tableau pour fournir le nom du site.

Options de connexion Tableau V3

Utilisez les options de connexion pour définir une connexion Tableau V3.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Par exemple :

```
./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="
```

Pour entrer plusieurs options, séparez-les par des espaces. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Tableau V3 obligatoires pour les commandes `infacmd isp CreateConnection` et `UpdateConnection` :

Propriété de connexion	Description
Produit Tableau	<p>Nom du produit Tableau auquel vous souhaitez vous connecter.</p> <p>Vous pouvez choisir l'un des produits Tableau suivants pour publier le fichier <code>.hyper</code> ou TWBX :</p> <p>Tableau Desktop</p> <p>Crée un fichier <code>.hyper</code> sur la machine qui exécute le service d'intégration de données. Vous pouvez ensuite importer manuellement le fichier <code>.hyper</code> dans Tableau Desktop.</p> <p>Tableau Server</p> <p>Publie le fichier <code>.hyper</code> ou TWBX généré dans Tableau Server.</p> <p>Tableau Online</p> <p>Publie le fichier <code>.hyper</code> ou TWBX généré dans Tableau Online.</p>
URL de connexion	<p>URL du produit Tableau Server ou Tableau Online sur lequel vous souhaitez publier le fichier <code>.hyper</code> ou TWBX.</p> <p>Entrez l'URL au format suivant : <code>http://<Host name of Tableau Server or Tableau Online>:<port></code></p>
Nom d'utilisateur	Nom d'utilisateur du compte Tableau Server ou Tableau Online.
Mot de passe	Mot de passe du compte Tableau Server ou Tableau Online.

Propriété de connexion	Description
ID du site	ID du site dans Tableau Server ou Tableau Online où vous souhaitez publier le fichier .hyper ou TWBX. Remarque: Contactez l'administrateur de Tableau pour fournir l'ID de site.
Chemin d'accès au fichier de schéma	Chemin d'accès à l'exemple de fichier .hyper à partir duquel le service d'intégration de données importe les métadonnées de Tableau. Entrez l'une des options suivantes pour le chemin d'accès au fichier de schéma : <ul style="list-style-type: none"> - Chemin d'accès absolu au fichier .hyper. - Chemin d'accès au répertoire des fichiers .hyper. - Chemin de répertoire vide. Le chemin que vous spécifiez pour le fichier de schéma devient le chemin par défaut du fichier .hyper cible. Si vous ne spécifiez pas un chemin d'accès au fichier, le service d'intégration de données utilise celui par défaut du fichier .hyper cible : <Data Integration Service installation directory>/apps/ Data_Integration_Server/<latest version>/bin/rtdm

Options de connexion Teradata Parallel Transporter

Utilisez les options de connexion pour définir une connexion Teradata PT.

Entrez les options de connexion au format suivant :

```
... -o option_name='value' option_name='value' ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Teradata PT pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
UserName	Requis. Nom d'utilisateur de la base de données Teradata disposant des autorisations d'écriture adéquates pour accéder à la base de données.
Mot de passe	Requis. Mot de passe du nom d'utilisateur de la base de données Teradata.
DriverName	Requis. Nom du pilote JDBC Teradata.
ConnectionString	Requis. URL JDBC permettant d'obtenir des métadonnées.
TDPID	Requis. Nom ou adresse IP de l'ordinateur de base de données Teradata.
databaseName	Requis. Nom de la base de données Teradata. Si vous n'entrez pas un nom de base de données, l'API Teradata PT utilise le nom de connexion de la base de données par défaut.
DataCodePage	Facultatif. Page de code associée à la base de données. Lorsque vous exécutez un mappage qui se charge vers une cible Teradata, la page de code de la connexion Teradata PT doit être identique à la page de code de la cible Teradata. La valeur par défaut est UTF-8.

Option	Description
Ténacité	Facultatif. Nombre d'heures pendant lesquelles l'API Teradata PT continue les tentatives de connexion lorsque le nombre de tentatives maximal d'opérations est atteint sur la base de données Teradata. Doit être un entier positif non nul. La valeur par défaut est 4.
MaxSessions	Facultatif. Nombre maximal de sessions que l'API Teradata PT établit avec la base de données Teradata. Doit être un entier positif non nul. La valeur par défaut est 4.
MinSessions	Facultatif. Le nombre minimal de sessions API Teradata PT requis pour que la tâche API Teradata PT continue. Doit être un entier positif entre 1 et la valeur du nombre de sessions maximal. La valeur par défaut est 1.
Veille	Facultatif. Nombre de minutes pendant lesquelles l'API Teradata PT se met en pause avant de tenter de se reconnecter lorsque le nombre maximal d'opérations sont en cours d'exécution sur la base de données Teradata. Doit être un entier positif non nul. La valeur par défaut est 6.
useMetadataJdbcUrl	Facultatif. Définissez cette option sur True pour indiquer que le connecteur Teradata pour Hadoop (TDCH) doit utiliser l'URL JDBC que vous avez spécifiée dans la chaîne de connexion. Définissez cette option sur False pour spécifier une autre URL JDBC que TDCH doit utiliser lorsqu'il exécute le mappage.
tdchJdbcUrl	Requis. URL JDBC que TDCH doit utiliser lorsqu'il exécute le mappage.
dataEncryption	Requis. Permet un cryptage de sécurité complet des demandes, des réponses et des données SQL sous Windows. Pour activer le cryptage des données sous UNIX, ajoutez la commande UseDataEncryption=Yes au DSN dans le fichier odbc.ini.
authenticationType	Requis. Authentifie l'utilisateur. Entrez les valeurs suivantes pour le type de l'authentification : <ul style="list-style-type: none"> - Native. Authentifie votre nom d'utilisateur et votre mot de passe par rapport à la base de données Teradata spécifiée dans la connexion. - LDAP. Authentifie les informations d'identification de l'utilisateur par rapport au service d'annuaire LDAP externe. La valeur par défaut est Native.

Option	Description
hadoopConnector	<p>Obligatoire si vous souhaitez activer la connectivité Sqoop pour l'objet de données qui utilise la connexion JDBC. Le service d'intégration de données exécute le mappage dans l'environnement d'exécution Hadoop via Sqoop.</p> <p>Vous pouvez configurer la connectivité Sqoop pour des objets de données relationnels, des objets de données personnalisés et des objets de données logiques qui sont basés sur une base de données compatible avec JDBC.</p> <p>Définissez la valeur sur <code>SQOOP_146</code> pour activer la connectivité Sqoop.</p>
hadoopConnectorArgs	<p>Facultatif. Entrez les arguments que le programme Sqoop doit utiliser pour se connecter à la base de données. Placez les arguments Sqoop entre guillemets simples. Séparez les arguments multiples par un espace.</p> <p>Par exemple, <code>hadoopConnectorArgs='--<Sqoop argument 1> --<Sqoop argument 2>'</code></p> <p>Pour lire des données depuis Teradata ou écrire des données dans Teradata par l'intermédiaire de connecteurs spécialisés TDCH (connecteur Teradata pour Hadoop) pour Sqoop, définissez la classe de fabrique de la connexion TDCH dans l'argument <code>hadoopConnectorArgs</code>. La classe de fabrique de la connexion dépend du connecteur Sqoop TDCH que vous souhaitez utiliser.</p> <ul style="list-style-type: none"> - Pour utiliser Cloudera Connector fourni par Teradata, configurez l'argument <code>hadoopConnectorArgs</code> de la manière suivante : <pre>hadoopConnectorArgs='- Dscoop.connection.factories=com.cloudera.connector.terad ata.TeradataManagerFactory'</pre> - Pour utiliser Hortonworks Connector for Teradata (fourni par Teradata Connector for Hadoop), configurez l'argument <code>hadoopConnectorArgs</code> de la manière suivante : <pre>hadoopConnectorArgs='- Dscoop.connection.factories=org.apache.sqoop.teradata.Te radataManagerFactory'</pre> <p>Si vous n'entrez aucun argument Sqoop, le service d'intégration de données construit la commande Sqoop en fonction des propriétés de connexion JDBC.</p>

Options de connexion Twitter

Utilisez les options de connexion pour définir une connexion Twitter.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Twitter pour les commandes `infacmd isp` `CreateConnection` et `UpdateConnection` :

Option	Description
ConsumerKey	La clé consommateur que vous obtenez lorsque vous créez l'application dans Twitter. Twitter utilise cette clé pour identifier l'application.
ConsumerSecret	Le secret du consommateur que vous obtenez lorsque vous créez l'application Twitter. Twitter utilise le secret pour établir la propriété de la clé du consommateur.
AccessToken	Jeton d'accès que l'utilitaire OAuth renvoie. Twitter utilise ce jeton au lieu des justificatifs d'identité de l'utilisateur pour accéder aux ressources protégées.
AccessSecret	Le secret d'accès que l'utilitaire OAuth renvoie. Le secret établit la propriété du jeton.

Options de connexion Twitter Streaming

Utilisez les options de connexion pour définir une connexion Twitter Streaming.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion Twitter Streaming pour les commandes `infacmd isp` `CreateConnection` et `UpdateConnection` :

Option	Description
HoseType	Méthodes de streaming d'API. Vous pouvez spécifier les méthodes suivantes : <ul style="list-style-type: none">- Filtre. La méthode <code>statuts/filtre</code> de Twitter renvoie les statuts publics qui correspondent aux critères de recherche.- Echantillon. La méthode <code>statuts/exemple</code> de Twitter renvoie un échantillon aléatoire de tous les statuts publics.
UserName	Le nom d'utilisateur Twitter qui apparaît à l'écran.
Mot de passe	Mot de passe Twitter.

Options de connexion VSAM

Utilisez les options de connexion pour définir une connexion VSAM.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion VSAM pour les commandes infacmd isp CreateConnection et UpdateConnection :

Option	Description
CodePage	Requis. Code pour lire à partir de ou écrire dans le fichier VSAM. Utilisez le nom de la page du code ISO, par exemple ISO-8859-6. Le nom de la page du code n'est pas sensible à la casse.
ArraySize	Facultatif. Détermine le nombre d'enregistrements dans la matrice de stockage pour les threads lorsque la valeur des threads de travail est supérieure à 0. Les valeurs valides sont comprises entre 1 et 5 000. La valeur par défaut est 25.
Compression	Facultatif. Compresse les données pour réduire le volume de données que les applications Informatica écrivent sur le réseau. True ou false. La valeur par défaut est False.
EncryptionLevel	Facultatif. Niveau de chiffrement. Si vous spécifiez AES pour l'option EncryptionType, spécifiez l'une des valeurs suivantes pour indiquer le niveau de chiffrement AES : <ul style="list-style-type: none"> - 1. Utilisez une clé de chiffrement 128 bits. - 2. Utilisez une clé de chiffrement 192 bits. - 3. Utilisez une clé de chiffrement 256 bits. La valeur par défaut est 1. Remarque: Si vous sélectionnez Aucun pour le type de chiffrement, le service d'intégration de données ignore la valeur de niveau de chiffrement.
EncryptionType	Facultatif. Vérifie s'il faut utiliser le chiffrement. Spécifiez l'une des valeurs suivantes : <ul style="list-style-type: none"> - Aucun - AES La valeur par défaut est Aucun.
InterpretAsRows	Facultatif. Si la valeur est « Vrai », la taille de stimulation représente un nombre de lignes. Si la valeur est False, la taille de stimulation représente des kilooctets. La valeur par défaut est False.
Emplacement	Emplacement du nœud d'écoute PowerExchange que vous pouvez connecter à VSAM. Le nœud est défini dans le fichier de configuration dbmover.cfg de PowerExchange.
OffLoadProcessing	Facultatif. Déplace le traitement des données en bloc depuis la machine VSAM à la machine du service d'intégration de données. Entrez l'une des valeurs suivantes : <ul style="list-style-type: none"> - Auto. Le service d'intégration de données détermine si vous souhaitez utiliser le traitement de déchargement. - Oui. Utiliser le traitement de déchargement. - Non. Ne pas utiliser le traitement de déchargement. La valeur par défaut est Auto.
PacingSize	Facultatif. Ralentit le taux de transfert de données pour réduire les goulets d'étranglement. Plus la valeur est basse, plus les performances de la session sont élevées. La valeur minimale est 0. Entrez 0 pour des performances optimales. La valeur par défaut est 0.
WorkerThread	Facultatif. Nombre de threads que le service d'intégration de données utilise pour traiter les données en bloc lorsque le traitement du déchargement est activé. Pour des performances optimales, cette valeur ne doit pas dépasser le nombre de processeurs disponibles sur la machine du service d'intégration de données. Les valeurs valides vont de 1 à 64. La valeur par défaut est 0, ce qui désactive le multithreading.

Option	Description
WriteMode	Entrez l'un des modes d'écriture suivants : - CONFIRMWRITEON. Envoie des données au service d'intégration de données et attend la réponse de réussite/échec avant d'envoyer davantage de données. - CONFIRMWRITEOFF. Envoie des données au service d'intégration de données sans attendre la réponse de réussite/échec. Utilisez cette option lorsque la table cible peut être rechargée si une erreur se produit. - ASYNCHRONOUSWITHFAULTT. Envoie des données au service d'intégration de données de manière asynchrone avec la possibilité de détecter les erreurs. La valeur par défaut est CONFIRMWRITEON.
EnableConnectionPool	Facultatif. Active le pooling de connexions. Lorsque vous activez le pooling de connexions, celui-ci conserve les instances de connexion inactives en mémoire. Lorsque vous désactivez le pooling de connexions, le service d'intégration de données arrête toute l'activité du pooling. True ou false. La valeur par défaut est False.
ConnectionPoolSize	Facultatif. Nombre maximal d'instances de connexion inactives que le service d'intégration de données gère pour une connexion de base de données. Définissez cette valeur à une valeur supérieure au nombre minimal d'instances de connexion inactives. La valeur par défaut est 15.
ConnectionPoolMaxIdle Time	Facultatif. Nombre de secondes pendant lesquelles une connexion qui dépasse le nombre minimal d'instances de connexion peut rester inactive avant que le pool de connexions ne l'abandonne. Le pool de connexions ignore la durée d'inactivité lorsque celle-ci ne dépasse pas le nombre minimal d'instances de connexion inactives. La valeur par défaut est 120.
ConnectionPoolMinConnections	Facultatif. Nombre minimal d'instances de connexion inactives que le pool maintient pour une connexion de base de données. Définissez cette valeur comme étant égale ou inférieure à la taille du pool de connexions inactives. La valeur par défaut est 0.

Options de connexion Web Content-Kapow Katalyst

Utilisez les options de connexion pour définir la connexion Web Content-Kapow Katalyst.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur qui contient un espace ou un autre caractère non alphanumérique, placez-la entre guillemets.

Le tableau suivant décrit les options de connexion Web Content-Kapow Katalyst pour les commandes infacmd isp CreateConnection et UpdateConnection commands :

Option	Description
ManagementConsoleURL	L'URL de la console de gestion locale sur laquelle le robot est chargé. L'URL doit commencer par http ou https. Par exemple : http://localhost:50080.
RQLServicePort	Le numéro de port où le service de socket guette le service RQL. Entrez une valeur entre 1 et 65 535. La valeur par défaut est 50 000.
Username	Nom d'utilisateur requis pour accéder à la console de gestion locale.
Password	Mot de passe pour accéder à la console de gestion locale.

CreateFolder

Crée un dossier dans le domaine. Lorsque vous créez un dossier, la commande infacmd crée le dossier dans le domaine ou le dossier que vous spécifiez.

Vous pouvez utiliser des dossiers pour organiser les objets et gérer la sécurité. Les dossiers peuvent contenir des nœuds, des services, des grilles, des licences et d'autres dossiers.

La commande infacmd isp CreateFolder utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp CreateFolder :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-FolderName -fn	folder_name	Requis. Nom du dossier. Les noms de dossier doivent être uniques dans un dossier ou le domaine. Ils ne peuvent pas contenir d'espaces ou dépasser 79 caractères.
-FolderPath -fp	full_folder_path	Requis. Chemin d'accès complet, sans le nom de domaine, de l'emplacement auquel vous souhaitez créer le dossier. Doit être au format suivant : <i>/parent_folder/child_folder</i>
-FolderDescription -fd	description_of_folder	Facultatif. Description du dossier. Si la description du dossier contient des espaces ou d'autres caractères non alphanumériques, placez-la entre guillemets.

CreateGrid

Crée une grille dans le domaine et assigne des nœuds à cette grille. Créez une grille pour distribuer des tâches à des processus de services exécutés sur des nœuds dans la grille.

La commande infacmd isp CreateGrid utilise la syntaxe suivante :

```
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]

```

Le tableau suivant décrit les options et arguments d'infacmd isp CreateGrid :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-GridName -gn	grid_name	Obligatoire. Nom de la grille.
-NodeList -nl	node1 node2 ...	Obligatoire. Noms des nœuds que vous souhaitez attribuer à la grille.
-FolderPath -fp	full_folder_path	Facultatif. Chemin d'accès complet, sans le nom de domaine, du dossier dans lequel vous souhaitez créer la grille. Doit être au format suivant : <i>/parent_folder/child_folder</i> La valeur par défaut est « / » (le domaine).

CreateGroup

Crée un groupe dans le domaine de sécurité natif. Vous pouvez assigner des rôles, autorisations et privilèges à un groupe dans le domaine de sécurité natif ou LDAP. Les rôles, autorisations et privilèges assignés au groupe déterminent les tâches que les utilisateurs du groupe peuvent effectuer dans le domaine.

La commande infacmd isp CreateGroup utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp CreateGroup :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-GroupName -gn	group_name	Obligatoire. Nom du groupe. Le nom du groupe n'est pas sensible à la casse et peut comporter de 1 à 80 caractères. Les tabulations, retours à la ligne et caractères spéciaux suivants ne sont pas admis : , + " \ < > ; / * % ? Le nom peut inclure des espaces ASCII, sauf en première et dernière positions. Tous les autres caractères d'espacement sont interdits.
-GroupDescription -ds	group_description	Facultatif. Description du groupe. Pour entrer une description qui contient des espaces ou d'autres caractères non alphanumériques, placez-la entre guillemets. La description ne peut pas inclure les caractères spéciaux suivants : < > "

CreateIntegrationService

Crée un service PowerCenter Integration Service dans un domaine.

Par défaut, le service PowerCenter Integration Service est activé lorsque vous le créez.

La commande `infacmd isp CreateIntegrationService` utilise la syntaxe suivante :

```
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]
```

Remarque: Pour infacmd isp CreateIntegrationService, vous ne devez pas utiliser les options -ru, -rp et -rsdn dans l'authentification Kerberos. Si vous utilisez ces options en mode Kerberos, la commande échoue.

Le tableau suivant décrit les options et arguments d'infacmd isp CreateIntegrationService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration PowerCenter. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas commencer ou se terminer par des espaces, contenir des retours chariot ou des tabulations, dépasser 79 caractères ou contenir les caractères suivants : / * ? < > "
-FolderPath -fp	full_folder_path	Facultatif. Chemin d'accès complet, sans le nom de domaine, du dossier dans lequel vous souhaitez créer le service d'intégration. Doit être au format suivant : <i>/parent_folder/child_folder</i> La valeur par défaut est « / » (le domaine).
-NodeName -nn	node_name	Obligatoire si vous ne spécifiez pas le nom de la grille. Nom du nœud sur lequel vous souhaitez que le processus de service d'intégration PowerCenter s'exécute. Si l'environnement PowerCenter est configuré pour une haute disponibilité, il s'agit du nom du nœud principal. Pour appliquer les modifications, redémarrez le service d'intégration.
-GridName -gn	grid_name	Obligatoire si vous ne spécifiez pas le nom du nœud. Nom de la grille sur laquelle vous souhaitez que le processus de service d'intégration PowerCenter s'exécute. Pour appliquer les modifications, redémarrez le service d'intégration PowerCenter.
-BackupNodes -bn	node1 node2 ...	Facultatif. Nœuds sur lesquels le processus de service peut s'exécuter lorsque le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.
-RepositoryService -rs	repository_service_name	Obligatoire. Nom du service de référentiel PowerCenter dont dépend le service d'intégration PowerCenter. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets. Pour appliquer les modifications, redémarrez le service d'intégration PowerCenter.

Option	Argument	Description
-RepositoryUser -ru	repository_user	Obligatoire pour l'authentification native ou LDAP. Nom d'utilisateur utilisé pour se connecter au référentiel PowerCenter. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets. Pour appliquer les modifications, redémarrez le service d'intégration PowerCenter.
-RepositoryPassword -rp	repository_password	Obligatoire pour l'authentification native ou LDAP. Mot de passe de l'utilisateur. Vous pouvez définir un mot de passe avec l'option -rp ou la variable d'environnement INFA_REPOSITORY_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -rp est prioritaire. Pour appliquer les modifications, redémarrez le service d'intégration PowerCenter.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Obligatoire pour LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel appartient l'utilisateur du référentiel PowerCenter. Le nom du domaine de sécurité est sensible à la casse. Si vous ne spécifiez pas cette option, la commande définit le domaine de sécurité de l'utilisateur du référentiel sur natif.
-ServiceDisable -sd	-	Facultatif. Crée un service désactivé. Vous devez activer le service pour pouvoir l'exécuter.
-ServiceOptions -so	option_name=value	Facultatif. Propriétés des services qui définissent la manière dont le service d'intégration PowerCenter est exécuté.
-ServiceProcessOptions -po	option_name=value	Facultatif. Propriétés du processus de service d'intégration PowerCenter. Dans une grille ou un environnement à plusieurs nœuds, infacmd applique ces propriétés au nœud principal, à la grille et au nœud de sauvegarde.
-EnvironmentVariables -ev	nom=valeur	Facultatif. Spécifiez les variables d'environnement comme options de processus de service d'intégration PowerCenter. Vous pouvez inclure des variables supplémentaires spécifiques à votre environnement PowerCenter. Pour appliquer les modifications, redémarrez le nœud.
-LicenseName -ln	license_name	Obligatoire si vous créez un service activé. Nom de la licence que vous souhaitez attribuer au service d'intégration PowerCenter. Pour appliquer les modifications, redémarrez le service d'intégration PowerCenter.

Options du service d'intégration

Entrez les options du service d'intégration au format suivant :

```
infacmd CreateIntegrationService ... -so option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options du service d'intégration :

Option	Description
\$PMFailureEmailUser	Facultatif. Adresse de courriel de l'utilisateur permettant de recevoir un courriel en cas d'échec d'une session. Pour entrer plusieurs adresses sous Windows, utilisez une liste de distribution. Pour entrer plusieurs adresses sous UNIX, séparez-les par une virgule.
\$PMSessionErrorThreshold	Facultatif. Nombre d'erreurs non fatales que le service d'intégration autorise avant de faire échouer la session. La valeur par défaut est 0 (les erreurs non fatales n'entraînent pas l'arrêt de la session).
\$PMSessionLogCount	Facultatif. Nombre de journaux de session que le service d'intégration archive pour la session. La valeur minimale est 0. La valeur par défaut est 0.
\$PMSuccessEmailUser	Facultatif. Adresse de courriel de l'utilisateur permettant de recevoir un courriel lorsqu'une session s'est correctement terminée. Pour entrer plusieurs adresses sous Windows, utilisez une liste de distribution. Pour entrer plusieurs adresses sous UNIX, séparez-les par une virgule.
\$PMWorkflowLogCount	Facultatif. Nombre de journaux de flux de travail que le service d'intégration archive pour le flux de travail. La valeur minimale est 0. La valeur par défaut est 0.
AggregateTreatNullAsZero	Facultatif. Traite les valeurs Null comme zéro dans les transformations Agrégation. La valeur par défaut est Non.
AggregateTreatRowAsInsert	Facultatif. Effectue des calculs agrégés avant de marquer les enregistrements en vue d'une insertion, d'une mise à jour, d'une suppression ou d'un rejet dans les expressions Stratégie de mise à jour. La valeur par défaut est Non.
ClientStore	Facultatif. Entrez la valeur pour ClientStore en utilisant la syntaxe suivante : <path>/<filename> Par exemple : ./Certs/client.keystore
CreateIndicatorFiles	Facultatif. Crée des fichiers indicateurs lorsque vous exécutez un flux de travail avec une cible de fichier plat. La valeur par défaut est Non.

Option	Description
DataMovementMode	Facultatif. Mode qui détermine comment le service d'intégration traite les données de caractères : <ul style="list-style-type: none"> - ASCII - Unicode La valeur par défaut est ASCII.
DateDisplayFormat	Facultatif. Format de date utilisé par le service d'intégration dans les entrées de journal. La valeur par défaut est DY MON DD HH 24:MI:SS YYYY.
DateHandling40Compatibility	Facultatif. Gère les dates comme dans PowerCenter 1.0/ PowerMart 4.0. La valeur par défaut est Non.
DeadlockSleep	Facultatif. Nombre de secondes avant que le service d'intégration ne tente à nouveau d'écrire dans une cible sur un interblocage de base de données. La valeur minimale est 0. La valeur maximale est 2592000. La valeur par défaut est 0 (recommencer l'écriture de la cible immédiatement).
ErrorSeverityLevel	Facultatif. Niveau minimal de journalisation d'erreurs pour les journaux du service d'intégration : <ul style="list-style-type: none"> - Fatale - Erreur - Avertissement - Informations - Trace - Déboguer La valeur par défaut est Informations.
ExportSessionLogLibName	Facultatif. Nom d'un fichier de bibliothèque externe permettant d'écrire des messages de journal de session.
FlushGMDWrite	Obligatoire si vous activez la récupération de session. Vide les données de récupération de session pour le fichier de récupération, de la mémoire tampon du système d'exploitation vers le disque. Spécifiez l'un des niveaux suivants : <ul style="list-style-type: none"> - Auto. Purge les données de récupération pour toutes les sessions en temps réel avec une source JMS ou WebSphere MQ et une cible non relationnelle. - Oui. Purge les données de récupération pour toutes les sessions. - Non. Ne purge pas les données de récupération. Sélectionnez cette option si vous disposez de systèmes externes hautement disponibles ou si vous avez besoin d'optimiser les performances. La valeur par défaut est Auto.
HttpProxyDomain	Facultatif. Domaine pour l'authentification.
HttpProxyPassword	Obligatoire si le serveur proxy requiert une authentification. Mot de passe pour l'utilisateur authentifié.
HttpProxyPort	Facultatif. Numéro de port du serveur proxy HTTP.

Option	Description
HttpProxyServer	Facultatif. Nom du serveur proxy HTTP.
HttpProxyUser	Obligatoire si le serveur proxy requiert une authentification. Nom d'utilisateur authentifié pour le serveur proxy HTTP.
IgnoreResourceRequirements	Facultatif. Ignore les besoins en ressources de tâches lors de la distribution de tâches aux nœuds d'une grille. La valeur par défaut est Oui.
JCEProvider	Facultatif. Nom de classe JCEProvider pour la prise en charge de l'authentification NTLM. Par exemple : <code>com.unix.crypto.provider.UnixJCE.</code>
JoinerSourceOrder6xCompatibility	Facultatif. Traite les pipelines principaux et secondaires par ordre séquentiel comme dans les versions de PowerCenter antérieures à la version 7.0. La valeur par défaut est Non.
LoadManagerAllowDebugging	Facultatif. Vous permet d'utiliser ce service d'intégration pour exécuter des sessions de débogage à partir du concepteur. La valeur par défaut est Oui.
LogInUTF8	Facultatif. Écrit tous les journaux en utilisant le jeu de caractères UTF-8. La valeur par défaut est Oui (Unicode) ou non (ASCII).
MSExchangeProfile	Facultatif. Profil Microsoft Exchange utilisé par le compte Démarrage du service pour envoyer un courriel après la session.
MaxLookupSPDBConnections	Facultatif. Nombre maximal de connexions à une base de données de recherche ou de procédures stockées lors du démarrage d'une session. La valeur minimale est 0. La valeur par défaut est 0.
MaxMSSQLConnections	Facultatif. Nombre maximal de connexions à une base de données Microsoft SQL Server lors du démarrage d'une session. La valeur minimale est 100. La valeur maximale est 2 147 483 647. La valeur par défaut est 100.
MaxResilienceTimeout	Facultatif. Délai maximal, en secondes, pendant lequel le service conserve les ressources à des fins de résilience. La valeur minimale est 0. La valeur maximale est 2592000. La valeur par défaut est 180.
MaxSybaseConnections	Facultatif. Nombre maximal de connexions à une base de données Sybase lors du démarrage d'une session. La valeur minimale est 100. La valeur maximale est 2 147 483 647. La valeur par défaut est 100.
NumOfDeadlockRetries	Facultatif. Nombre de fois que le service d'intégration retente d'écrire dans une cible sur un interblocage de base de données. La valeur minimale est 10. La valeur maximale est 1 000 000 000. La valeur par défaut est 10.

Option	Description
OperatingMode	Facultatif. Mode de fonctionnement du service d'intégration : <ul style="list-style-type: none"> - Normal - Sécurisé La valeur par défaut est Normal.
OperatingModeOnFailover	Facultatif. Mode de fonctionnement du service d'intégration lorsque le processus de service bascule : <ul style="list-style-type: none"> - Normal - Sécurisé La valeur par défaut est Normal.
OutputMetaDataForFF	Facultatif. Écrit les en-têtes de colonne dans les cibles de fichiers plats. La valeur par défaut est Non.
PersistRuntimeStatsToRepo	Facultatif. Niveau des informations d'exécution stockées dans le référentiel. Spécifiez l'un des niveaux suivants : <ul style="list-style-type: none"> - Aucun. Le service d'intégration ne stocke pas d'informations d'exécution de session ou de flux de travail dans le référentiel. - Normal. Le service d'intégration stocke les détails du flux de travail, les détails de la tâche, les statistiques de la session et les statistiques de la source et de la cible dans le référentiel. - Commentaires prolixes. Le service d'intégration stocke les détails du flux de travail, les détails de la tâche, les statistiques de la session, les détails de la partition et les détails de performance dans le référentiel. La valeur par défaut est Normal.
Pmservice3XCompatibility	Facultatif. Gère les transformations Agrégation comme le faisait le serveur PowerMart dans PowerMart 3.5. La valeur par défaut est Non.
RunImpactedSessions	Facultatif. Exécute des sessions concernées par les mises à jour de dépendances. La valeur par défaut est Non.
ServiceResilienceTimeout	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. La valeur minimale est 0. La valeur maximale est 2592000. La valeur par défaut est 180.
StoreHAPersistenceInDB	Facultatif. Stocke les informations d'état de processus dans des tables persistantes de la base de données du référentiel PowerCenter associé. La valeur par défaut est Non.
TimestampWorkflowLogMessages	Facultatif. Ajoute un horodatage aux messages écrits dans le journal de flux de travail. La valeur par défaut est Non.
TreatCharAsCharOnRead	Facultatif. Conserve les espaces de fin lors de la lecture de données CHAR SAP ou PeopleSoft. La valeur par défaut est Oui.
TreatDBPartitionAsPassThrough	Facultatif. Utilise un partitionnement d'intercommunication pour les cibles autres que DB2 lorsque le type de partition est Partitionnement de base de données. La valeur par défaut est Non.

Option	Description
TreatNullInComparisonOperatorsAs	Facultatif. Détermine comment le service d'intégration évalue les valeurs Null dans les opérations de comparaison : <ul style="list-style-type: none"> - Null - Faible - Élevée La valeur par défaut est Null.
TrustStore	Facultatif. Entrez la valeur de TrustStore selon la syntaxe suivante : <path>/<filename> Par exemple : ./Certs/trust.keystore
UseOperatingSystemProfiles	Facultatif. Permet l'utilisation de profils de système d'exploitation. Utilisez cette option si le service d'intégration est exécuté sous UNIX.
ValidateDataCodePages	Facultatif. Applique la compatibilité de la page de code des données. La valeur par défaut est Oui.
WriterWaitTimeOut	Facultatif. Dans le mode de validation basé sur les cibles, durée en secondes pendant laquelle le programme d'écriture reste inactif avant d'émettre une validation lorsque les conditions suivantes sont remplies : <ul style="list-style-type: none"> - Le PowerCenter Integration Service a écrit les données dans la cible. - Le PowerCenter Integration Service n'a pas émis de validation. Le service d'intégration PowerCenter peut valider la cible avant ou après l'intervalle de validation configuré. La valeur minimale est 60. La valeur maximale est 2592000. La valeur par défaut est 60.
XMLWarnDupRows	Facultatif. Écrit des avertissements de lignes dupliquées et des lignes dupliquées pour les cibles XML dans le journal de session. La valeur par défaut est Oui.

Options du processus de service d'intégration

Entrez les options de processus de service au format suivant :

```
infacmd CreateIntegrationService ... -po option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options du processus de service d'intégration :

Option	Description
\$PMBadFileDir	Facultatif. Répertoire par défaut pour les fichiers de rejet. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/BadFiles.
\$PMCacheDir	Facultatif. Répertoire par défaut pour les fichiers d'index et de cache de données. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/Cache.
\$PMExtProcDir	Facultatif. Répertoire par défaut pour les procédures externes. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/ExtProc.
\$PMLookupFileDir	Facultatif. Répertoire par défaut pour les fichiers de recherche. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/LkpFiles.
\$PMRootDir	Facultatif. Répertoire racine accessible par le nœud. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est C:\Informatica\PowerCenter8.6\server\infa_shared.
\$PMSessionLogDir	Facultatif. Répertoire par défaut pour les journaux de sessions. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/SessLogs.
\$PMSourceFileDir	Facultatif. Répertoire par défaut pour les fichiers source. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/SrcFiles.
\$PMStorageDir	Facultatif. Répertoire par défaut pour les fichiers d'exécution. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/Storage.
\$PMTargetFileDir	Facultatif. Répertoire par défaut pour les fichiers cible. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/TgtFiles.
\$PMTempDir	Facultatif. Répertoire par défaut pour les fichiers temporaires. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/Temp.

Option	Description
\$PMWorkflowLogDir	Facultatif. Répertoire par défaut pour les journaux de flux de travail. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/WorkflowLogs.
Codepage_ID	Obligatoire. Numéro de l'ID de page de code pour le processus de service d'intégration.
JVMClassPath	Facultatif. Chemin de classe Java SDK.
JVMMaxMemory	Facultatif. Quantité maximale de mémoire que le Java SDK utilise au cours d'une session PowerCenter. La valeur par défaut est 64 Mo.
JVMMinMemory	Facultatif. Quantité minimale de mémoire que le Java SDK utilise au cours d'une session PowerCenter. La valeur par défaut est 32 Mo.

CreateMMService

Crée un service Metadata Manager dans le domaine. Par défaut, le service Metadata Manager est désactivé lorsque vous le créez. Exécutez `infacmd EnableService` pour activer le service Metadata Manager.

La commande `infacmd isp CreateMMService` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp CreateMMService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-ServiceName -sn	service_name	Obligatoire. Nom du service Metadata Manager. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Le nom ne peut pas contenir des espaces, des retours chariot ou des tabulations, dépasser 79 caractères ou inclure les caractères suivants : / * ? < > "
-NodeName -nn	node_name	Obligatoire. Nom du nœud où vous voulez que l'application Metadata Manager soit exécutée.
-ServiceOptions -so	option_name=value	Facultatif. Propriétés du service qui définissent la manière d'exécuter le service de gestionnaire de métadonnées.
-LicenseName -ln	license_name	Obligatoire. Nom de la licence que vous voulez assigner au service de gestionnaire de métadonnées.
-FolderPath -fp	full_folder_path	Facultatif. Chemin d'accès complet, sans le nom de domaine, du dossier dans lequel vous souhaitez créer le service Metadata Manager. Doit être au format suivant : <i>/parent_folder/child_folder</i> La valeur par défaut est « / » (le domaine).

Options du service Metadata Manager

Entrez les options du service Metadata Manager au format suivant :

```
infacmd isp CreateMMService ... -so option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur qui contient un espace ou un autre caractère non alphanumérique, placez-la entre guillemets.

Le tableau suivant décrit les options du service Metadata Manager :

Option	Description
AgentPort	Obligatoire. Numéro de port de l'agent Metadata Manager. L'agent utilise ce port pour communiquer avec des référentiels de métadonnées source. La valeur par défaut est 10 251.
CodePage	Obligatoire. Page de code de la description pour le service d'archives Metadata Manager. Pour saisir une description de page de code qui contient un espace ou un autre caractère non-alphanumérique, placez son nom entre guillemets.
ConnectionString	Obligatoire. Chaîne de connexion native de la base de données du service d'archives Metadata Manager.
DBUser	Obligatoire. Compte utilisateur de la base de données du service d'archives Metadata Manager.

Option	Description
DBPassword	Obligatoire. Mot de passe d'utilisateur de la base de données du service d'archives Metadata Manager. Mot de passe de l'utilisateur. Vous pouvez définir un mot de passe avec l'option -so ou la variable d'environnement INFA_DEFAULT_DATABASE_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -so est prioritaire.
DatabaseHostname	Obligatoire. Nom d'hôte de la base de données du service d'archives Metadata Manager.
DatabaseName	Obligatoire. Nom du service complet ou SID pour les bases de données Oracle. Nom du service pour les bases de données IBM DB2. Nom de la base de données pour la base de données Microsoft SQL Server.
DatabasePort	Obligatoire. Numéro de port de la base de données du service d'archives Metadata Manager.
DatabaseType	Obligatoire. Type de base de données du service d'archives Metadata Manager.
ErrorSeverityLevel	Facultatif. Niveau des messages d'erreur inscrits dans le journal du service Metadata Manager. La valeur par défaut est ERROR.
FileLocation	Obligatoire. Emplacement des fichiers utilisés par l'application Metadata Manager.
JdbcOptions	Facultatif. Options JDBC supplémentaires. Vous pouvez utiliser cette propriété pour indiquer les informations suivantes : <ul style="list-style-type: none"> - Emplacement du serveur de sauvegarde - Paramètres de l'option de sécurité avancée Oracle (ASO) - Paramètres d'authentification Microsoft SQL Server - Paramètres JDBC supplémentaires lorsque la communication sécurisée est activée pour la base de données du référentiel Metadata Manager Pour plus d'informations sur ces paramètres, consultez le <i>Guide Informatica Application Service</i> .
MaxConcurrentRequests	Facultatif. Nombre maximal de threads de traitement de demandes disponibles, ce qui détermine le nombre maximal de demandes clients pouvant être gérées simultanément par Metadata Manager. La valeur par défaut est 100.
MaxHeapSize	Facultatif. Quantité de mémoire vive, en mégaoctets, attribuée au Gestionnaire virtuel Java (JVM) qui exécute le Metadata Manager. La valeur par défaut est 512.
MaxQueueLength	Facultatif. Longueur de queue maximale des demandes de connexion entrantes lorsque tous les threads de traitement de demande possibles sont utilisés par l'application Metadata Manager. La valeur par défaut est 500.
MaximumActiveConnections	Facultatif. Nombre de connexions actives disponibles dans la base de données du service d'archives Metadata Manager. L'application Metadata Manager maintient un pool de connexions pour les connexions à la base de données du référentiel. La valeur par défaut est 20.
MaximumWaitTime	Facultatif. Durée en secondes pendant laquelle Metadata Manager interrompt les demandes de connexion à la base de données dans le pool de connexions. La valeur par défaut est 180.
MetadataTreeMaxFolderChilds	Facultatif. Nombre d'objets enfants disponibles dans le catalogue de métadonnées Metadata Manager pour tout objet parent. La valeur par défaut est 100.

Option	Description
ODBCConnectionMode	Mode de connexion utilisé par le service d'intégration pour se connecter aux sources de métadonnées et au service d'archives Metadata Manager lors du chargement des ressources. Les valeurs peuvent être « Vrai » ou « Faux ». Vous devez définir cette propriété comme « Vrai » si le service d'intégration est exécuté sur une machine UNIX et que vous voulez charger les métadonnées depuis une base de données Microsoft SQL Server ou si vous utilisez une base de données Microsoft SQL Server pour le service d'archives Metadata Manager.
OracleConnType	Obligatoire si vous sélectionnez Oracle comme type de base de données. Type de connexion Oracle. Vous pouvez entrer l'une des options suivantes : - OracleSID - OracleServiceName
PortNumber	Obligatoire. Numéro de port sur lequel l'application Metadata Manager est exécutée. La valeur par défaut est 10 250.
StagePoolSize	Facultatif. Nombre maximum de ressources que Metadata Manager peut charger simultanément. La valeur par défaut est 3.
TablespaceName	Nom de l'espace de table d'un service d'archives Metadata Manager sur IBM DB2.
TimeoutInterval	Facultatif. Durée en minutes pendant laquelle Metadata Manager maintient le chargement des ressources ayant échoué dans la file d'attente de chargement. La valeur par défaut est 30.
URLScheme	Obligatoire. Indique le protocole de sécurité que vous configurez pour l'application Metadata Manager : HTTP ou HTTPS.
keystoreFile	Obligatoire si vous utilisez HTTPS. Fichier entrepôt de clés contenant les clés et les certificats obligatoire si vous utilisez le protocole de sécurité SSL avec l'application Metadata Manager.

CreateOSProfile

Crée un profil de système d'exploitation dans le domaine. Avant de pouvoir exécuter des flux de travail utilisant des profils de système d'exploitation, vous devez configurer le service d'intégration PowerCenter pour utiliser ces profils.

La commande `infacmd isp CreateOSProfile` utilise la syntaxe suivante :

```
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 ...]

```

Le tableau suivant décrit les options et arguments d'infacmd isp CreateOSProfile :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-OSProfileName -on	OSProfile_name	Requis. Nom du profil de système d'exploitation. Le nom du profil de système d'exploitation peut comporter jusqu'à 80 caractères. Il ne peut pas inclure d'espaces ou les caractères spéciaux suivants : % * + \ / ? ; < >
-SystemName -sn	system_username	Requis. Nom d'un utilisateur du système d'exploitation qui existe sur les machines sur lesquelles le service d'intégration s'exécute. Le service d'intégration exécute les flux de travail à l'aide de l'accès système de l'utilisateur système défini pour le profil de système d'exploitation.
- IntegrationServiceProcessOptions -po	option_name=value	Facultatif. Propriétés de service qui définissent le mode d'exécution du service d'intégration PowerCenter.
-EnvironmentVariables -ev	nom=valeur	Facultatif. Nom et valeur des variables d'environnement utilisées par le service d'intégration PowerCenter lors de l'exécution.
-DISProcessVariables -diso	option_name=value	Facultatif. Propriétés du processus de service qui définissent le mode d'exécution du service d'intégration de données.

Option	Argument	Description
-DISEnvironmentVariables -dis	nom=valeur	Facultatif. Nom et valeur des variables d'environnement utilisées par le service d'intégration de données lors de l'exécution.
-HadoopImpersonationProperties -hipr	hadoop_impersonation_properties	Facultatif. Indique si le service d'intégration de données utilise l'utilisateur d'emprunt d'identité Hadoop pour exécuter des mappages, des flux de travail et des tâches de profilage dans un environnement Hadoop. Les valeurs valides sont True ou False.
-HadoopImpersonationUser -hu	hadoop_impersonation_user	Facultatif. Entrez le nom d'utilisateur dont le service d'intégration de données emprunte l'identité lorsqu'il exécute des tâches dans un environnement Hadoop.
-UseLoggedInUserAsProxy -ip	use_logged_in_user_as_proxy	Facultatif. Indique si vous souhaitez utiliser l'utilisateur connecté en tant qu'utilisateur d'emprunt d'identité Hadoop. Les valeurs valides sont True ou False.
-ProductExtensionName -pe	product_extension_name	Facultatif. Réserve pour une utilisation ultérieure.
-ProductOptions -o	optionGroupName.optionName=Value	<p>Obligatoire. Nom et valeur de chaque option définie. Utilisez l'option permettant de créer un répertoire du cache de fichier plat que le profil du système d'exploitation peut utiliser.</p> <p>Par exemple, la commande suivante définit le répertoire du cache sur \$PMRootDir/OSPCache:</p> <pre>infacmd isp createOSProfile ... -o 'runTimeVariables.flatFileCacheDirectory'=" \$PMRootDir/OSPCache"</pre>

Options des processus de service d'intégration de données pour les profils de système d'exploitation

Entrez les options de processus de service d'intégration de données au format suivant :

```
infacmd CreateOSProfile ... -diso option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options du processus de service d'intégration de données :

Option	Description
\$DISRootDir	Répertoire racine auquel le nœud peut accéder. Il s'agit du répertoire racine d'autres variables de processus de service. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , []
\$DISTempDir	Répertoire des fichiers temporaires créés lors de l'exécution des tâches. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , [] La valeur par défaut est <répertoire racine>/disTemp. Remarque: Si le service d'intégration de données est configuré de manière à utiliser plusieurs profils de système d'exploitation, spécifiez un répertoire commun pour tous les profils, car un répertoire distinct pour chaque profil entraîne une utilisation excessive de l'espace disque.
\$DISCacheDir	Répertoire des fichiers d'index et de cache de données des transformations. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , [] La valeur par défaut est <répertoire racine>/cache.
\$DISSourceDir	Répertoire des fichiers plats sources utilisés dans un mappage. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , [] La valeur par défaut est <répertoire racine>/source.
\$DISTargetDir	Répertoire des fichiers plats cibles utilisés dans un mappage. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , [] La valeur par défaut est <répertoire racine>/cible.
\$DISRejectedFilesDir	Répertoire des fichiers de rejet. Les fichiers de rejet contiennent des lignes qui ont été rejetées lors de l'exécution d'un mappage. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , [] La valeur par défaut est <répertoire racine>/rejet.
\$DISLogDir	Répertoire des journaux. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , [] La valeur par défaut est <répertoire racine>/disLogs.

Options des processus de service d'intégration PowerCenter pour les profils de système d'exploitation

Entrez les options de processus du service d'intégration PowerCenter au format suivant :

```
infacmd CreateOSProfile ... -po option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de processus du service d'intégration PowerCenter :

Option	Description
\$PMBadFileDir	Facultatif. Répertoire des fichiers de rejet. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/BadFiles.
\$PMCacheDir	Facultatif. Répertoire des fichiers d'index et de cache de données. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/Cache.
\$PMExtProcDir	Facultatif. Répertoire des procédures externes. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/ExtProc.
\$PMLookupFileDir	Facultatif. Répertoire des fichiers de recherche. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/LkpFiles.
\$PMRootDir	Facultatif. Répertoire racine auquel le nœud peut accéder. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est C:\Informatica\PowerCenter\server\infa_shared.
\$PMSessionLogDir	Facultatif. Répertoire des journaux de sessions. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/SessLogs.
\$PMSourceFileDir	Facultatif. Répertoire des fichiers sources. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/SrcFiles.
\$PMStorageDir	Facultatif. Répertoire des fichiers d'exécution. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/Storage.
\$PMTargetFileDir	Facultatif. Répertoire des fichiers cibles. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/TgtFiles.
\$PMTempDir	Facultatif. Répertoire des fichiers temporaires. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/Temp.

CreateRepositoryService

Crée un service de référentiel PowerCenter dans un domaine.

Par défaut, le service de référentiel PowerCenter est activé lors de sa création.

Un service de référentiel PowerCenter gère un référentiel. Il effectue toutes les transactions de métadonnées entre le référentiel et les clients du référentiel.

La commande infacmd isp CreateRepositoryService utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp CreateRepositoryService :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel PowerCenter. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas commencer ou se terminer par des espaces, contenir des retours chariot ou des tabulations, dépasser 79 caractères ou contenir les caractères suivants : \ / : * ? < > "
-NodeName -nn	node_name	Requis. Nom du nœud sur lequel vous souhaitez exécuter le processus de service du référentiel PowerCenter. Si l'environnement PowerCenter est configuré pour une haute disponibilité, il s'agit du nom du nœud principal.
-BackupNodes -bn	node1 node2 ...	Facultatif. Nœuds sur lesquels le processus de service peut s'exécuter lorsque le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.
-ServiceDisable -sd	-	Facultatif. Crée un service désactivé. Vous devez activer le service pour pouvoir l'exécuter.

Option	Argument	Description
-ServiceOptions -so	option_name=value	Requis. Propriétés du service qui définissent le mode d'exécution du service de référentiel PowerCenter.
-LicenseName -ln	license_name	Obligatoire si vous créez un service activé. Nom de la licence que vous souhaitez attribuer au service de référentiel PowerCenter.
-FolderPath -fp	full_folder_path	Facultatif. Chemin d'accès complet, sans le nom de domaine, du dossier dans lequel vous souhaitez créer le service de référentiel PowerCenter. Doit être au format suivant : <i>/parent_folder/child_folder</i> La valeur par défaut est « / » (le domaine).

Options de service de référentiel (-so)

Entrez les options de service de référentiel au format suivant :

```
infacmd CreateRepositoryService ... -so option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options du service de référentiel :

Option	Description
AllowWritesWithRACaching	Facultatif. Utilise les outils clients PowerCenter pour modifier les métadonnées du référentiel lorsque la mise en cache de RepAgent est activée. La valeur par défaut est Oui.
CheckinCommentsRequired	Facultatif. Les utilisateurs doivent ajouter des commentaires lors de l'archivage d'objets du référentiel. La valeur par défaut est Oui. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.
CodePage	Requis. Description de la page de code de la base de données. Pour saisir une description de page de code contenant une espace ou tout autre caractère non alphanumérique, placez son nom entre guillemets.
ConnectionString	Requis. Chaîne de connexion de la base de données spécifiée lors de la configuration du service de référentiel PowerCenter. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.
DBPassword	Requis. Mot de passe de l'utilisateur de la base de données du référentiel. Vous pouvez définir un mot de passe avec l'option -so ou la variable d'environnement INFA_DEFAULT_DATABASE_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -so est prioritaire. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.
DBPoolExpiryThreshold	Facultatif. Nombre minimal de connexions de base de données inactives autorisé par le service de référentiel PowerCenter. Par exemple, si 20 connexions sont inactives et que vous réglez ce seuil sur 5, le service de référentiel PowerCenter ne ferme pas plus de 15 connexions. La valeur minimale est 3. La valeur par défaut est 5.

Option	Description
DBPoolExpiryTimeout	Facultatif. Intervalle, en secondes, pendant lequel le service de référentiel PowerCenter recherche des connexions de base de données inactives. Si une connexion est inactive pour une durée supérieure à cette valeur, le service de référentiel PowerCenter peut fermer la connexion. La valeur minimale est 300. La valeur maximale est 2 592 000 (30 jours). La valeur par défaut est 3 600 (1 heure).
DBUser	Requis. Compte de la base de données contenant le référentiel. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.
DatabaseArrayOperationSize	Facultatif. Nombre de lignes à récupérer à chaque opération sur une base de données de tableau (insertion ou récupération, par exemple). La valeur par défaut est 100. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.
DatabaseConnectionTimeout	Facultatif. Temps en secondes pendant lequel le service de référentiel PowerCenter tente d'établir une connexion au système de gestion de base de données. La valeur par défaut est 180.
DatabasePoolSize	Facultatif. Nombre maximal de connexions à la base de données du référentiel que le service de référentiel PowerCenter est capable d'établir. La valeur minimale est 20. La valeur par défaut est 500.
DatabaseType	Requis. Type de base de données qui contient les métadonnées du référentiel. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.
EnableRepAgentCaching	Facultatif. Active la fonctionnalité de mise en cache de l'agent du référentiel. La valeur par défaut est Oui.
ErrorSeverityLevel	Facultatif. Niveau minimal des messages d'erreur écrits dans le journal du service de référentiel PowerCenter : <ul style="list-style-type: none"> - Irrécupérable - Erreur - Avertissement - Informations - Trace - Déboguer La valeur par défaut est Informations.
HeartBeatInterval	Facultatif. Intervalle pendant lequel le service de référentiel PowerCenter vérifie sa connexion aux clients du service. La valeur par défaut est 60 secondes.
MaxResilienceTimeout	Facultatif. Délai maximal, en secondes, pendant lequel le service conserve les ressources à des fins de résilience. La valeur par défaut est 180.
MaximumConnections	Facultatif. Nombre maximal de connexions que le référentiel accepte des clients du référentiel. La valeur par défaut est 200.
MaximumLocks	Facultatif. Nombre maximal de verrous que le référentiel place sur les objets de métadonnées. La valeur par défaut est 50 000.

Option	Description
OperatingMode	<p>Facultatif. Mode d'exécution du service de référentiel PowerCenter :</p> <ul style="list-style-type: none"> - Normal - Exclusif <p>La valeur par défaut est Normal. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.</p>
OptimizeDatabaseSchema	<p>Facultatif. Permet d'optimiser le schéma de base de données du référentiel lors de la création du contenu du référentiel ou de la sauvegarde et de la restauration d'un référentiel IBM DB2 ou Microsoft SQL Server. Une fois activé, le service de référentiel PowerCenter tente de créer les tables de référentiel qui contiennent des colonnes Varchar avec une précision de 2000 au lieu de colonnes CLOB. Utilisez les colonnes Varchar pour augmenter les performances du référentiel. Lors de l'utilisation des colonnes Varchar, vous devez réduire les entrées et sorties disque et la base de données peut mettre les colonnes en cache.</p> <p>Pour utiliser cette option, vérifiez la taille de page requise pour les bases de données de référentiel suivantes :</p> <ul style="list-style-type: none"> - IBM DB2. La taille de page de la base de données doit être supérieure ou égale à 4 Ko. Au minimum, un espace de table temporaire ayant une taille de page supérieure ou égale à 16 Ko. - Microsoft SQL Server. La taille de page de la base de données doit être supérieure ou égale à 8 Ko. <p>La valeur par défaut est désactivée.</p>
PreserveMXData	<p>Facultatif. Conserve les données MX pour les versions antérieures des mappages. La valeur par défaut est désactivée.</p>
RACacheCapacity	<p>Facultatif. Nombre d'objets que le cache peut contenir lorsque la mise en cache de l'agent du référentiel est activée. La valeur par défaut est 10 000.</p>
SecurityAuditTrail	<p>Facultatif. Permet le suivi des modifications apportées aux utilisateurs, aux groupes, aux privilèges et aux autorisations. La valeur par défaut est Non.</p>
ServiceResilienceTimeout	<p>Facultatif. Période (en secondes) pendant laquelle le service tente d'établir ou de rétablir une connexion à un autre service. La valeur par défaut est 180. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.</p>
TableOwnerName	<p>Facultatif. Nom du propriétaire des tables de référentiel pour un référentiel IBM DB2.</p>
TablespaceName	<p>Facultatif. Nom de l'espace de table pour les référentiels IBM DB2. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.</p>
TrustedConnection	<p>Facultatif. Utilise l'authentification Windows pour accéder à la base de données Microsoft SQL Server. La valeur par défaut est Non. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.</p>

CreateRole

Crée un rôle personnalisé dans le domaine. Vous pouvez alors assigner des privilèges au rôle pour le domaine ou pour un type de service d'application. Vous ne pouvez pas créer de rôles définis par le système.

La commande infacmd isp CreateRole utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp CreateRole :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-RoleName -rn	role_name	Obligatoire. Nom du rôle. Le nom de rôle est sensible à la casse et peut comporter de 1 à 80 caractères. Les tabulations, retours à la ligne et caractères spéciaux suivants ne sont pas admis : , + " \ < > ; / * % ? Le nom peut inclure des espaces ASCII, sauf en première et dernière positions. Tous les autres caractères d'espacement sont interdits.
-RoleDescription -rd	role_description	Facultatif. Description du rôle. La description peut comporter un maximum de 1 000 caractères et ne peut pas inclure de tabulations, de retours à la ligne ou les caractères spéciaux suivants : < > " Pour entrer une description qui contient des espaces ou d'autres caractères non alphanumériques, placez-la entre guillemets.

CreateSAPBWService

Crée un service SAP BW dans le domaine. Par défaut, le service SAP BW est activé lorsque vous le créez.

La commande infacmd isp CreateSAPBWService utilise la syntaxe suivante :

```
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]

```

Le tableau suivant décrit les options et arguments d'infacmd isp CreateSAPBWService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Obligatoire. Nom du service SAP BW. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas commencer ou se terminer par des espaces, contenir des retours chariot ou des tabulations, dépasser 79 caractères ou contenir les caractères suivants : / * ? < > "
-NodeName -nn	node_name	Obligatoire. Nom du nœud sur lequel vous souhaitez que le processus de service SAP BW s'exécute. Si l'environnement PowerCenter est configuré pour une haute disponibilité, il s'agit du nom du nœud principal.
-IntegrationService -is	integration_service_name	Obligatoire. Nom du service d'intégration auquel le service SAP BW se connecte. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.

Option	Argument	Description
-RepositoryUser -ru	user	Obligatoire. Nom d'utilisateur utilisé pour la connexion au référentiel. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-RepositoryPassword -rp	mot de passe	Obligatoire si la communication sécurisée n'est pas activée pour le domaine. Facultatif si la communication sécurisée est activée pour le domaine. Mot de passe de l'utilisateur. Vous pouvez définir un mot de passe avec l'option -rp ou la variable d'environnement INFA_REPOSITORY_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -rp est prioritaire.
-ServiceOptions -so	option_name=value	Facultatif. Propriétés du service qui définissent le mode d'exécution du service SAP BW.
-ServiceProcessOptions -po	option_name=value	Facultatif. Propriétés du processus de service pour le service SAP BW.
-ServiceDisable -sd	-	Facultatif. Crée un service désactivé. Vous devez activer le service pour pouvoir l'exécuter.
-LicenseName -ln	license_name	Obligatoire si vous créez un service activé. Nom de la licence que vous souhaitez attribuer au service SAP BW.
-FolderPath -fp	full_folder_path	Facultatif. Chemin d'accès complet, sans le nom de domaine, du dossier dans lequel vous souhaitez créer le service SAP BW. Doit être au format suivant : <i>/parent_folder/child_folder</i> La valeur par défaut est « / » (le domaine).

Options du service SAP BW

Entrez les options du service SAP BW au format suivant :

```
infacmd CreateSAPBWService ... -so option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options du service SAP BW :

Option	Description
BWSystemConxString	Facultatif. Entrée DEST définie dans le fichier <code>sapnwrfc.ini</code> pour une connexion à un programme de serveur RFC. Modifiez cette propriété si vous avez créé une autre entrée DEST dans le fichier <code>sapnwrfc.ini</code> pour le service SAP BW.
RetryPeriod	Facultatif. Délai d'attente en secondes du service SAP BW avant une nouvelle tentative de connexion au système BW en cas d'échec d'une tentative précédente. La valeur par défaut est 5.

Option de processus de service SAP BW

Entrez l'option de processus de service au format suivant :

```
infacmd CreateSAPBWService ... -po option_name=value
```

Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit l'option de processus de service SAP BW :

Option	Description
ParamFileDir	Facultatif. Répertoire du fichier de paramètres temporaire. La valeur par défaut est <code>/Infa_Home/server/infa_shared/BWParam</code> .

CreateUser

Crée un compte utilisateur dans le domaine de sécurité natif. Vous pouvez alors attribuer des rôles, des autorisations et des privilèges à un compte utilisateur. Les rôles, autorisations et privilèges attribués à l'utilisateur déterminent les tâches que l'utilisateur peut effectuer dans le domaine.

La syntaxe de la commande `infacmd isp CreateUser` est la suivante :

```
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]

Le tableau suivant décrit les options et arguments d'infacmd isp CreateUser :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NewUserName -nu	new_user_name	Obligatoire. Nom de connexion du compte utilisateur. Le nom de connexion d'un compte utilisateur doit être unique dans le domaine de sécurité auquel il appartient. Le nom de connexion n'est pas sensible à la casse et peut comprendre de 1 à 80 caractères. Les tabulations, retours à la ligne et caractères spéciaux suivants ne sont pas admis : , + " \ < > ; / * & % ? Le nom peut inclure des espaces ASCII, sauf en première et dernière position. Tous les autres caractères d'espacement sont interdits.
-NewUserPassword -np	new_user_password	Obligatoire. Mot de passe du compte utilisateur. Vous pouvez définir un mot de passe avec l'option -np ou la variable d'environnement INFA_PASSWORD. Si vous définissez un mot de passe avec ces deux méthodes, le mot de passe défini par l'option -np est prioritaire. Pour un compte utilisateur natif, si vous activez la complexité du mot de passe, utilisez les directives suivantes lorsque vous créez ou modifiez un mot de passe : <ul style="list-style-type: none"> - Le mot de passe doit contenir au moins huit caractères. - Il doit être composé d'un caractère alphabétique, d'un caractère numérique et d'un caractère non alphanumérique, tels que : ! \ " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { } ~ Lorsque vous utilisez des caractères spéciaux dans un mot de passe, il arrive que l'interpréteur de commandes les lise différemment. Par exemple, \$ est interprété comme une variable. Dans ce cas, utilisez un caractère d'échappement pour échapper le caractère spécial.
-NewUserFullName -nf	new_user_full_name	Facultatif. Nom complet du compte utilisateur. Pour entrer un nom qui contient des espaces ou d'autres caractères non alphanumériques, placez-le entre guillemets. Le nom complet ne peut pas inclure les caractères spéciaux suivants : < > "
-NewUserDescription -ds	new_user_description	Facultatif. Description du compte utilisateur. Pour entrer une description qui contient des espaces ou d'autres caractères non alphanumériques, placez-la entre guillemets. La description ne peut pas inclure les caractères spéciaux suivants : < > "

Option	Argument	Description
-NewUserEmailAddress -em	new_user_email_address	Facultatif. Adresse de courriel de l'utilisateur. Pour entrer une adresse qui contient des espaces ou d'autres caractères non alphanumériques, placez-la entre guillemets. L'adresse de courriel ne peut pas inclure les caractères spéciaux suivants : < > " Entrez l'adresse de courriel au format UserName@Domain.
-NewUserPhoneNumber -pn	new_user_phone_number	Facultatif. Numéro de téléphone de l'utilisateur. Pour entrer un numéro de téléphone qui contient des espaces ou d'autres caractères non alphanumériques, placez-le entre guillemets. Le numéro de téléphone ne peut pas inclure les caractères spéciaux suivants : < > "

CreateWSHubService

Crée un Hub de services Web dans le domaine. Par défaut, le Hub de services Web est activé lorsque vous le créez.

La commande infacmd isp CreateWSHubService utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp CreateWSHubService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-ServiceName -sn	service_name	Nom du hub de services Web que vous souhaitez créer. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas commencer ou se terminer par des espaces, contenir des retours chariot ou des tabulations, dépasser 79 caractères ou contenir les caractères suivants : / * ? < > "
-FolderPath -fp	full_folder_path	Facultatif. Chemin d'accès complet, sans le nom de domaine, du dossier dans lequel vous souhaitez créer le hub de services Web. Doit être au format suivant : <i>/parent_folder/child_folder</i> La valeur par défaut est « / » (le domaine).
-NodeName -nn	node_name	Obligatoire. Nom du nœud sur lequel vous souhaitez que le processus du hub de services Web s'exécute.
-RepositoryService -rs	repository_service_name	Obligatoire. Nom du service de référentiel dont dépend le hub de services Web. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-RepositoryUser -ru	repository_user	Obligatoire. Nom d'utilisateur utilisé pour la connexion au référentiel. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-RepositoryPassword -rp	repository_password	Obligatoire. Mot de passe de l'utilisateur. Vous pouvez définir un mot de passe avec l'option -rp ou la variable d'environnement INFA_REPOSITORY_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -rp est prioritaire.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Obligatoire si le domaine utilise l'authentification LDAP ou l'authentification Kerberos. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel appartient l'utilisateur du référentiel PowerCenter. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ServiceDisable -sd	-	Facultatif. Crée un service désactivé. Vous devez activer le service pour pouvoir l'exécuter.

Option	Argument	Description
-ServiceOptions -so	option_name=value ...	Facultatif. Propriétés du service qui définissent le mode d'exécution du hub de services Web.
-LicenseName -ln	license_name	Obligatoire. Nom de la licence que vous souhaitez attribuer au hub de services Web.

Options du Hub de services Web

Entrez les options du Hub de services Web dans le format suivant :

```
infacmd CreateWSHubService ... -so option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options du Hub de services Web :

Option	Description
DTMTimeout	Facultatif. Temps en secondes pris par <i>infacmd</i> pour tenter d'établir ou rétablir une connexion au DTM. Par défaut 60.
ErrorSeverityLevel	Facultatif. Le niveau minimum de journalisation d'erreur pour le Hub de services Web : <ul style="list-style-type: none"> - Fatale - Erreur - Avertissement - Informations - Trace - Déboguer La valeur par défaut est Informations.
HubHostName	Facultatif. Nom de la machine hébergeant le Hub de services Web. Valeur par défaut : localhost. Pour appliquer les modifications, redémarrez le Hub de services Web.
HubPortNumber(http)	Facultatif. Numéro de port sur lequel est exécuté le Hub de services Web dans Tomcat. Par défaut 7333. Pour appliquer les modifications, redémarrez le Hub de services Web.
HubPortNumber (https)	Numéro de port sur lequel est exécuté le Hub de services Web dans Tomcat. Requis en cas d'exécution du Hub de services Web sur HTTPS. Par défaut 7343.
InternalHostName	Facultatif. Nom d'hôte sur lequel le Hub de services Web écoute les connexions à partir du service d'intégration. Valeur par défaut : localhost. Pour appliquer les modifications, redémarrez le Hub de services Web.
InternalPortNumber	Facultatif. Numéro de port sur lequel le Hub de services Web écoute les connexions à partir du service d'intégration. Par défaut 15555. Pour appliquer les modifications, redémarrez le Hub de services Web.

Option	Description
MaxConcurrentRequests	Facultatif. Nombre maximum de threads de traitement de demande disponibles, qui détermine le nombre maximum de demandes simultanées pouvant être gérées. Par défaut 100.
MaxLMConnections	Facultatif. Nombre maximum de connexions au service d'intégration pouvant être ouverts à la fois pour Web Services Hub. Par défaut 20.
MaxQueueLength	Facultatif. Longueur de queue maximale des demandes de connexion entrantes lorsque tous les threads de traitement de demande possibles sont utilisés. Par défaut 5000.
SessionExpiryPeriod	Facultatif. Durée en secondes pendant laquelle une session peut rester inutilisée avant que son ID de session ne devienne invalide. La valeur par défaut est de 3600 secondes.
URLScheme	Facultatif. Protocole de sécurité que vous configurez pour Web Services Hub : HTTP ou HTTPS. Valeur par défaut : HTTP. Pour appliquer les modifications, redémarrez le Hub de services Web.
WSH_ENCODING	Facultatif. Codage de caractères du Hub de services Web. La valeur par défaut est UTF-16LE. Pour appliquer les modifications, redémarrez le Hub de services Web.
KeystoreFile	Facultatif. Le fichier entrepôt de clés contient les clés et les certificats requis pour utiliser le protocole de sécurité SSL avec le Hub de services Web.

DeleteNamespace

Supprime un domaine de sécurité LDAP et les utilisateurs et groupes du domaine de sécurité. Supprime le domaine de sécurité LDAP si le domaine Informatica utilise l'authentification LDAP ou Kerberos.

La commande `infacmd` `isp DeleteNamespace` utilise la syntaxe suivante :

```

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

```

Le tableau suivant décrit les options et les arguments d'infacmd isp DeleteNamespace :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité que vous voulez créer et auquel l'utilisateur du domaine appartient. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Vous pouvez spécifier une valeur pour -sdn ou utiliser la valeur par défaut selon le mode d'authentification : <ul style="list-style-type: none"> - Obligatoire si le domaine utilise l'authentification LDAP. La valeur par défaut est Natif. Pour travailler avec l'authentification LDAP, vous devez spécifier la valeur pour -sdn. - Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. La valeur par défaut est natif pour l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd essaye d'établir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous ne spécifiez pas la variable d'environnement, la valeur par défaut utilisée est de 180 secondes.
-NameSpace -ns	espace de nom	Obligatoire. Nom du domaine de sécurité LDAP ou Kerberos. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Le nom ne peut pas contenir d'espaces ou les caractères spéciaux suivants : , + / < > @ ; \ % ? Le nom ne peut pas dépasser 128 caractères. Le nom peut inclure des espaces ASCII, sauf en première et dernière position. Vous ne pouvez pas utiliser d'autres caractères d'espace.

DisableNodeResource

Désactive une ressource Informatica. Les ressources Informatica incluent les ressources de répertoire de fichiers, les ressources personnalisées et les ressources de connexion. Désactivez les ressources non disponibles pour empêcher l'équilibrage de charge de répartir une tâche sur un nœud ne disposant pas des ressources requises.

Vous pouvez désactiver les ressources de répertoire de fichiers, les ressources personnalisées et les ressources de connexion.

Quand un service d'intégration PowerCenter est exécuté sur une grille, l'équilibrage de charge peut utiliser des ressources pour distribuer des tâches Session, Command et Event-wait prédéfinies. Si service d'intégration PowerCenter est configuré pour vérifier les ressources, l'équilibrage de charge distribue les tâches aux nœuds avec les ressources disponibles.

Par défaut, toutes les ressources de connexion sont activées sur un nœud.

La commande infacmd isp DisableNodeResource utilise la syntaxe suivante :

```
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

Le tableau suivant décrit les options et arguments d'infacmd isp DisableNodeResource :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NodeName -nn	node_name	Requis. Nom du nœud sur lequel la ressource est définie.

Option	Argument	Description
-ResourceCategory -rc	resource_category	Facultatif. Catégorie de la ressource. Les catégories valides incluent : - PCIS. Ressource pour le service d'intégration PowerCenter. - DIS. Réserve pour un usage futur. La valeur par défaut est PCIS.
-ResourceType -rt	resource_type	Requis. Type de ressource. Les types valides comprennent : - Personnalisé - Répertoire de fichier - Connexion
-ResourceName -rn	resource_name	Requis. Nom complet de la ressource. Pour répertorier les noms de toutes les ressources disponibles pour un nœud, exécutez la commande infacmd isp ListNodeResources.

DisableService

Désactive le service d'application correspondant au nom du service. Lorsque vous désactivez un service, tous les processus de services s'arrêtent.

Désactive un type de service d'application, y compris les services système.

La commande infacmd isp DisableService utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp DisableService :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-ServiceName -sn	service_name	Requis. Nom du service que vous souhaitez désactiver. Pour entrer un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-Mode -mo	disable_mode	Requis. Définit le mode désactivation du service : <ul style="list-style-type: none"> - Terminer. Désactive le service lorsque tous les processus de service sont arrêtés. - Arrêter. Si le service est un service d'intégration PowerCenter, interrompt tous les flux de travail en cours d'exécution et désactive le service d'intégration PowerCenter. Si le service est un service Analyst, interrompt toutes les tâches, puis désactive le service. - Abandonner. Interrompt immédiatement tous les processus, puis désactive le service.

Remarque: Si vous spécifiez un mode de désactivation Stop pour un service d'écoute, la commande attend jusqu'à 30 secondes que le service d'écoute termine les sous-tâches puis éteint le service et le processus du service d'écoute.

DisableServiceProcess

Désactive le processus de service sur un nœud spécifié.

Vous pouvez désactiver un processus de service sur un nœud spécifié si le nœud requiert une maintenance.

La commande infacmd isp DisableServiceProcess utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp DisableServiceProcess :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Obligatoire. Nom du service associé au processus que vous souhaitez désactiver. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.

Option	Argument	Description
-NodeName -nn	node_name	Obligatoire. Nom du nœud sur lequel le processus de service est en cours d'exécution.
-Mode -mo	disable_mode	Obligatoire. Définit la manière dont le processus de service est désactivé : <ul style="list-style-type: none"> - Terminer. Permet au processus de service de terminer les tâches en cours avant la désactivation. - Arrêter. Dans le cas d'un processus de service d'intégration, interrompt tous les flux de travail en cours d'exécution, puis désactive le processus. - Abandonner. Désactive le processus de service avant l'achèvement de la tâche en cours.

DisableUser

Désactive un compte utilisateur dans le domaine. Si vous ne souhaitez pas qu'un utilisateur accède au domaine temporairement, vous pouvez désactiver le compte utilisateur.

Lorsque vous désactivez un compte utilisateur, l'utilisateur ne peut pas se connecter aux applications de PowerCenter.

La commande infacmd isp DisableUser utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp DisableUser :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
ExistingUserName -eu	existing_user_name	Obligatoire. Compte utilisateur que vous souhaitez désactiver. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur que vous souhaitez désactiver. La valeur par défaut est Natif.

EditUser

Modifie les propriétés générales d'un compte utilisateur dans le domaine de sécurité natif.

Vous ne pouvez pas modifier les propriétés des comptes utilisateur dans le domaine de sécurité LDAP.

Vous ne pouvez pas changer le nom de connexion d'un utilisateur natif.

La commande infacmd isp EditUser utilise la syntaxe suivante :

```

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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp EditUser :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ExistingUserName -eu	existing_user_name	Obligatoire. Compte utilisateur que vous souhaitez modifier.
-ExistingUserFullName -sf	existing_user_full_name	Facultatif. Nom complet modifié du compte utilisateur. Pour saisir un nom qui contient des espaces ou d'autres caractères non alphanumériques, placez-le entre guillemets. Le nom complet ne peut pas inclure les caractères spéciaux suivants : < > "
-ExistingUserDescription -ds	existing_user_description	Facultatif. Description modifiée du compte utilisateur. Pour entrer une description qui contient des espaces ou d'autres caractères non alphanumériques, placez-la entre guillemets. La description ne peut pas inclure les caractères spéciaux suivants : < > "
-ExistingUserEmailAddress -em	existing_user_email_address	Facultatif. Adresse de courriel modifiée de l'utilisateur. Pour entrer une adresse qui contient des espaces ou d'autres caractères non alphanumériques, placez-la entre guillemets. L'adresse de courriel ne peut pas inclure les caractères spéciaux suivants : < > "
-ExistingUserPhoneNumber -pn	existing_user_phone_number	Facultatif. Numéro de téléphone modifié de l'utilisateur. Pour entrer un numéro de téléphone qui contient des espaces ou d'autres caractères non alphanumériques, placez-le entre guillemets. Le numéro de téléphone ne peut pas inclure les caractères spéciaux suivants : < > "

EnableNodeResource

Active une ressource Informatica. Les ressources Informatica incluent les fichiers ou les répertoires, les ressources personnalisées et les ressources de connexion. Lorsque vous activez une ressource sur un nœud, vous autorisez l'équilibrage de charge à distribuer des tâches nécessitant la ressource sur ce nœud.

Quand un service d'intégration PowerCenter est exécuté sur une grille, l'équilibrage de charge peut utiliser des ressources pour distribuer des tâches Session, Command et Event-wait prédéfinies. Si le service d'intégration PowerCenter est configuré pour vérifier des ressources, l'équilibrage de charge distribue des tâches aux nœuds où les ressources sont ajoutées et activées.

La commande `infacmd isp EnableNodeResource` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'`infacmd isp EnableNodeResource` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NodeName -nn	node_name	Requis. Nom du nœud sur lequel la ressource est définie.
-ResourceCategory -rc	resource_category	Facultatif. Catégorie de la ressource. Les catégories valides incluent : - PCIS. Ressource pour le service d'intégration PowerCenter. - DIS. Réserve pour un usage futur. La valeur par défaut est PCIS.
-ResourceType -rt	resource_type	Requis. Type de ressource. Les types valides comprennent : - Personnalisé - Répertoire de fichier - Connexion
-ResourceName -rn	resource_name	Requis. Nom complet de la ressource. Pour répertorier les noms de toutes les ressources disponibles pour un nœud, exécutez la commande ListNodeResources.

EnableService

Active le service d'application correspondant au nom du service.

Active tout type de service d'application, y compris les services système. Vous pouvez également activer Informatica Administrator.

La commande `infacmd isp EnableService` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'`infacmd isp EnableService` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Requis. Nom du service que vous souhaitez activer. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets. Pour démarrer l'outil Administrator, entrez _adminconsole.

EnableServiceProcess

Active un processus de service sur un nœud spécifié.

La commande infacmd isp EnableServiceProcess utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp EnableServiceProcess :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Obligatoire. Nom du service associé au processus que vous souhaitez activer. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-NodeName -nn	node_name	Obligatoire. Nom du nœud pour lequel vous souhaitez activer un processus de service.

EnableUser

Active un compte utilisateur dans le domaine.

La commande infacmd isp EnableUser utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp EnableUser :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.</p>
ExistingUserName -eu	existing_user_name	Obligatoire. Compte utilisateur que vous souhaitez activer. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur que vous souhaitez activer. La valeur par défaut est Natif.

ExportDomainObjects

Exporte les utilisateurs natifs, les groupes natifs, les rôles, les connexions et les configurations de cluster du domaine Informatica vers un fichier XML.

Si vous ne souhaitez pas exporter tous les objets du domaine, utilisez le fichier de contrôle d'exportation infacmd pour filtrer les objets à exporter.

Utilisez les commandes ExportDomainObjects et ImportDomainObjects pour migrer des objets entre deux domaines différents de la même version. Pour exporter des utilisateurs et groupes natifs à partir de domaines de versions différentes, utilisez la commande infacmd isp ExportUsersAndGroups.

Lorsque vous exportez un groupe, vous exportez tous les sous-groupes et utilisateurs de ce groupe.

Vous ne pouvez pas exporter l'utilisateur administrateur, le groupe d'administrateurs, les utilisateurs du groupe d'administrateurs, le groupe Tout le monde ou les utilisateurs ou groupes LDAP. Pour répliquer des utilisateurs et groupes LDAP dans un domaine Informatica, importez-les directement à partir du service d'annuaire LDAP.

Si la commande échoue et renvoie une erreur de mémoire Java, augmentez la mémoire système disponible pour infacmd. Pour augmenter la mémoire système, définissez la valeur -Xmx dans la variable d'environnement ICMD_JAVA_OPTS.

La syntaxe de la commande infacmd isp ExportDomainObjects est la suivante :

```
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>]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ExportDomainObjects :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire. Pour un compte utilisateur natif, si vous activez la complexité du mot de passe, utilisez les directives suivantes lorsque vous créez ou modifiez un mot de passe : <ul style="list-style-type: none"> - Le mot de passe doit contenir au moins huit caractères. - Il doit être composé d'un caractère alphabétique, d'un caractère numérique et d'un caractère non alphanumérique, tels que : <pre>! \ " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { } ~</pre> Lorsque vous utilisez des caractères spéciaux dans un mot de passe, il arrive que l'interpréteur de commandes les lise différemment. Par exemple, \$ est interprété comme une variable. Dans ce cas, utilisez un caractère d'échappement pour échapper le caractère spécial.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ExportFile -fp	export_file_name	Obligatoire. Chemin et nom du fichier d'exportation. Si vous ne spécifiez pas le chemin du fichier, infacmd crée le fichier dans le répertoire où vous exécutez la commande infacmd.
-ExportControlFile -cp	export_control_file	Facultatif. Nom et chemin du fichier de contrôle d'exportation qui filtre les objets exportés.
-RetainPassword -rp	retain_password	Facultatif. Défini sur « True » pour conserver des mots de passe cryptés pour les utilisateurs et les connexions dans le fichier exporté. Lorsqu'il est défini sur « False », les mots de passe utilisateur et de connexion sont exportés en tant que chaînes vides. La valeur par défaut est False.
-Force -f	-	Facultatif. Remplace le fichier d'exportation si un fichier du même nom existe déjà. Si vous omettez cette option, la commande vous demande confirmation avant d'écraser le fichier.

ExportUsersAndGroups

Exporte des utilisateurs et des groupes natifs vers un fichier XML.

Si la commande échoue et renvoie une erreur de mémoire Java, augmentez la mémoire système disponible pour infacmd. Pour augmenter la mémoire système, définissez la valeur -Xmx dans la variable d'environnement ICMD_JAVA_OPTS.

La syntaxe de la commande infacmd isp ExportUsersAndGroups est la suivante :

```
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>]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ExportUsersAndGroups :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	password	<p>Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p> <p>Pour un compte utilisateur natif, si vous activez la complexité du mot de passe, utilisez les directives suivantes lorsque vous créez ou modifiez un mot de passe :</p> <ul style="list-style-type: none"> - Le mot de passe doit contenir au moins huit caractères. - Il doit être composé d'un caractère alphabétique, d'un caractère numérique et d'un caractère non alphanumérique, tels que : <pre>! \ " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { } ~</pre> <p>Lorsque vous utilisez des caractères spéciaux dans un mot de passe, il arrive que l'interpréteur de commandes les lise différemment. Par exemple, \$ est interprété comme une variable. Dans ce cas, utilisez un caractère d'échappement pour échapper le caractère spécial.</p>
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port...	<p>Obligatoire si les informations de connectivité de passerelle du fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.</p>

Option	Argument	Description
-ExportFile -ef	export_file_name	Obligatoire. Nom et chemin de l'emplacement auquel vous souhaitez écrire le fichier d'exportation. Si vous ne spécifiez pas le chemin du fichier, infacmd crée le fichier de sauvegarde dans le répertoire où vous exécutez la commande infacmd.
-Force -f	-	Facultatif. Remplace le fichier d'exportation si un fichier du même nom existe déjà. Si vous omettez cette option, la commande vous demande confirmation avant de supprimer le fichier.

LIENS CONNEXES :

- [“ImportUsersAndGroups” à la page 579](#)

GetFolderInfo

Obtenez des informations sur les dossiers. Les informations sur les dossiers incluent leurs chemin, nom et description.

Pour exécuter la commande infacmd isp GetFolderInfo, vous devez avoir l'autorisation sur le dossier.

La commande infacmd isp GetFolderInfo utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp GetFolderInfo :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-FolderPath -fp	full_folder_path	Obligatoire. Chemin d'accès complet du dossier sans le nom de domaine. Doit être au format suivant : <i>/parent_folder/child_folder</i>

GetLastError

Obtient les messages d'erreur les plus récents pour un service d'application s'exécutant sur un nœud.

Les messages d'erreur sont les événements du journal dont le niveau de gravité est *erreur* ou *fatal*. Cette commande ne renvoie aucune erreur survenue avant le dernier démarrage des services Informatica.

Vous pouvez obtenir des messages d'erreur dans un fichier ou les afficher à l'écran.

La commande infacmd isp GetLastError utilise la syntaxe suivante :

```
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]
```


Le tableau suivant décrit les options et arguments d'infacmd isp GetLastError :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Facultatif. Nom du service pour lequel vous souhaitez obtenir des messages d'erreur. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.

Option	Argument	Description
-NodeName -nn	node_name	Obligatoire. Nom du nœud sur lequel s'exécute le service.
-Format -fm	format	Facultatif. Format des messages d'erreur. Les types valides comprennent : - Text - XML Si vous ne spécifiez pas de format, infacmd affiche les messages au format texte avec des lignes limitées à 80 caractères.
-MaxEvents -me	maximum_number_of_error_events	Facultatif. Nombre maximal de messages d'erreur à obtenir. La valeur par défaut est 1. La valeur maximum est 20.

GetLog

Obtient les événements de journaux. Vous pouvez obtenir les événements de journaux pour un domaine ou des services. Vous pouvez écrire des événements de journaux dans un fichier ou les afficher à l'écran.

Pour obtenir les événements de journaux pour un domaine, vous devez avoir l'autorisation sur le domaine. Pour obtenir les événements de journaux pour un service, vous devez avoir l'autorisation sur le service.

La commande infacmd isp GetLog utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp GetLog :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-StartDate -sd	start_date_time	<p>Facultatif. Renvoie les événements de journaux à partir de ces date et heure. Entrez la date et l'heure dans l'un des formats suivants :</p> <ul style="list-style-type: none"> - MM/dd/yyyy_hh:mm:ssa_Z - MM/dd/yyyy_hh:mm:ssa_Z - MM/dd/yyyy_hh:mm:ssa - MM/dd/yyyy_hh:mm:ssa - yyyy-MM-dd_HH:mm:ss_Z - yyyy-MM-dd_HH:mm:ss_Z - yyyy-MM-dd_HH:mm:ss - yyyy-MM-dd_HH:mm:ss - MM/dd/yyyy hh:mm:ssa Z - MM/dd/yyyy hh:mm:ssa Z - MM/dd/yyyy hh:mm:ssa - MM/dd/yyyy hh:mm:ssa - yyyy-MM-dd HH:mm:ss_Z - yyyy-MM-dd HH:mm:ss_Z - yyyy-MM-dd HH:mm:ss - yyyy-MM-dd HH:mm:ss - MM/dd/yyyy - yyyy-MM-dd <p>Où « a » est un marqueur am/pm (« a » pour am (avant midi) et « p » pour pm (après midi)) et « z » un marqueur de fuseau horaire (par exemple, « -0800 » ou « GMT »).</p>
-EndDate -ed	end_date_time	<p>Facultatif. Renvoie les événements de journaux qui se terminent à ces date et heure. Entrez la date et l'heure au même format que l'option StartDate.</p> <p>Si vous entrez une date de fin qui est antérieure à la date de début, GetLog ne renvoie aucun événement de journaux.</p>
-ReverseOrder -ro	-	Facultatif. Obtient les événements de journaux selon l'horodatage le plus récent.
-Format -fm	format	<p>Facultatif. Format des événements de journaux. Les types valides comprennent :</p> <ul style="list-style-type: none"> - Texte - XML - Bin (binaire) <p>Si vous choisissez le format binaire, vous devez spécifier un nom de fichier à l'aide de l'option OutputFile.</p> <p>Si vous ne spécifiez aucun format, infacmd utilise le format texte avec des lignes limitées à 80 caractères.</p>

Option	Argument	Description
-OutputFile -lo	output_file_name	Nom et chemin de l'emplacement dans lequel vous souhaitez écrire le fichier journal. Par défaut, le gestionnaire de service utilise le répertoire server\infa_shared\log sur le nœud principal de passerelle. Omettez cette option pour afficher les événements de journaux à l'écran. Si vous choisissez le type de fichier de sortie binaire, vous devez spécifier un nom de fichier à l'aide de cette option.
-ServiceType -st	service_type	Facultatif. Type de service pour lequel vous souhaitez obtenir les événements de journaux. Vous pouvez spécifier un type de service. Omettez cette option pour obtenir les événements de journaux pour tous les types de service. Les types de services comprennent : <ul style="list-style-type: none"> - AS. Service Analyst - BW. Service SAP BW - CMS. Service de gestion de contenu - DIS. Service d'intégration de données - ES. Service de messagerie électronique - IS. Service d'intégration PowerCenter - MM. Service Metadata Manager - MRS. Service de référentiel modèle - RMS. Service de gestionnaire de ressource - RS. Service de référentiel PowerCenter - SCH. Service de planificateur - SEARCH. Service de recherche - TDM. Service Test Data Manager - TDW. Service Test Data Warehouse - WS. Hub des services Web - DOMAIN. Domaine
-ServiceName -sn	service_name	Facultatif. Nom du service pour lequel vous souhaitez obtenir les événements de journaux. Pour entrer un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-Severity -svt	severity_level	Facultatif. Gravité du message. Les types de gravité incluent : <ul style="list-style-type: none"> - Fatale - Erreur - Avertissement - Informations - Trace - Déboguer

GetNodeName

Renvoie le nom d'un nœud.

Obtient le nom de nœud depuis le fichier nodemeta.xml sur le nœud. Vous devez entrer cette commande sur le nœud dont vous souhaitez extraire le nom.

La commande `infacmd isp GetNodeName` utilise la syntaxe suivante :

```
GetNodeName  
[<-OutputFile|-o>] output_file
```

Lorsque vous utilisez la commande sans l'option `-o`, la commande imprime le nom du nœud dans la fenêtre de commande. Lorsque vous utilisez l'option `-o` pour spécifier un fichier de sortie, vous indiquez le nom et le chemin du fichier. Par exemple :

```
isp\bin\infacmd.bat getNodeName -o c:\node_name.txt
```

La commande crée un fichier `node_name.txt` dans le chemin que vous spécifiez. Elle imprime le nom du nœud dans le fichier. Si le fichier existe, la commande le remplace.

GetPasswordComplexityConfig

Renvoie la configuration de complexité du mot de passe pour les utilisateurs du domaine.

La syntaxe de la commande `infacmd GetPasswordComplexityConfig` est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd GetPasswordComplexityConfig` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option <code>-dn</code> ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option <code>-dn</code> est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option <code>-un</code> ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option <code>-un</code> est prioritaire.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option <code>-pd</code> ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option <code>-pd</code> est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Spécifiez les noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire. La valeur par défaut est 180 secondes.

getDomainSamlConfig

Renvoie le statut de l'authentification SAML (Secure Assertion Markup Language) pour un domaine Informatica. Si l'authentification SAML est activée, la commande renvoie également l'URL du fournisseur d'identité et la différence de temps autorisée entre l'horloge du système hôte du fournisseur d'identité et celle du nœud principal de passerelle.

Exécutez la commande sur l'un des nœuds de passerelle du domaine Informatica. Vous devez disposer du rôle d'administrateur pour pouvoir exécuter cette commande.

La commande `infacmd isp getDomainSamlConfig` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd isp getDomainSamlConfig` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, <code>infacmd</code> utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

GetServiceOption

Obtient la valeur d'une propriété du service pour le service d'intégration PowerCenter, le service de référentiel PowerCenter, le service SAP BW ou encore le service Hub des services Web. Pour les options de service d'intégration de données ou de service Analyst, exécutez la commande infacmd dis ou infacmd en tant que ListServiceOptions.

Par exemple, vous pouvez extraire le type de base de données de référentiel.

La commande infacmd isp GetServiceOption utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp GetServiceOption :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Obligatoire. Nom du service pour lequel vous souhaitez obtenir une valeur. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-OptionName -op	option_name	Obligatoire. Nom de l'option pour laquelle vous souhaitez récupérer une valeur. Les options que vous indiquez dépendent du type de service : <ul style="list-style-type: none"> - Pour plus d'informations sur ces options du service d'intégration, consultez "Options du service d'intégration" à la page 488. - Pour un service SAP BW, spécifiez « BWSysConXString » (la destination SAP - Type R) ou « RetryPeriod » (la période de nouvelle tentative en secondes). - Pour plus d'informations sur les options du hub de services Web, consultez "Options du Hub de services Web" à la page 520.

GetServiceProcessOption

Obtient la valeur pour une propriété lorsqu'un processus de service d'intégration PowerCenter s'exécute sur un nœud.

La commande infacmd isp GetServiceProcessOption utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et arguments d'infacmd isp GetServiceProcessOption :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Obligatoire. Nom du service pour lequel vous souhaitez obtenir une valeur. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-NodeName -nn	node_name	Obligatoire. Nom du nœud sur lequel le processus de service est en cours d'exécution.
-OptionName -op	option_name	Obligatoire. Nom de l'option pour laquelle vous souhaitez récupérer une valeur.

LIENS CONNEXES :

- [“Options du processus de service d'intégration” à la page 492](#)

GetServiceProcessStatus

Obtient le statut d'un processus de service d'application sur un nœud. Un processus de service peut être activé ou désactivé.

La commande infacmd isp GetServiceProcessStatus utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp GetServiceProcessStatus :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-ServiceName -sn	service_name	Obligatoire. Nom du service qui exécute le processus dont vous souhaitez connaître le statut. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-NodeName -nn	node_name	Obligatoire. Nom du nœud sur lequel le processus de service est en cours d'exécution.

GetServiceStatus

Obtient le statut d'un service d'application.

Vous pouvez extraire le statut d'un service tel que le service de référentiel, le service d'intégration de données, le service Analyst, le service d'intégration, Hub de services Web ou le service SAP BW. Un service peut être activé ou désactivé.

La commande infacmd isp GetServiceStatus utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp GetServiceStatus :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Obligatoire. Nom du service dont vous souhaitez connaître le statut. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.

GetSessionLog

Obtient les événements du journal pour la dernière exécution d'une session. Le service de référentiel PowerCenter doit être en cours d'exécution lorsque vous exécutez cette commande.

La commande infacmd isp GetSessionLog utilise la syntaxe suivante :

```
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

```

Remarque: Si vous ne spécifiez pas les options -un, -pd et -sdn, la commande infacmd isp GetSessionLog utilise les valeurs correspondantes des options -ru, -rp et -rsdn.

Le tableau suivant décrit les options et arguments d'infacmd isp GetSessionLog :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-Format -fm	format	Facultatif. Format du journal de session. Les types valides comprennent : <ul style="list-style-type: none"> - Text - XML - Bin (binaire) Si vous choisissez le format binaire, vous devez spécifier un nom de fichier à l'aide de l'option OutputFile. Si vous ne spécifiez aucun format, <i>infacmd</i> utilise le format texte avec des lignes limitées à 80 caractères.
-OutputFile -lo	output_file_name	Nom et chemin du fichier journal de session. Par défaut, le gestionnaire de service utilise le répertoire server\infa_shared\log sur le nœud principal de passerelle. Omettez cette option pour afficher les événements du journal à l'écran. Si vous choisissez le type de fichier de sortie binaire, vous devez spécifier un nom de fichier à l'aide de cette option.
-IntegrationService -is	integration_service_name	Obligatoire. Nom du service d'intégration qui exécute la session. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-RepositoryService -rs	repository_service_name	Obligatoire. Nom du service de référentiel qui contient la session. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.

Option	Argument	Description
-RepositoryDomain -rd	domain_of_repository	Obligatoire si le référentiel ne se trouve pas dans le domaine local. Domaine du service de référentiel. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-RepositoryUser -ru	repository_user	Obligatoire pour l'authentification native ou LDAP. Facultatif si le domaine utilise l'authentification Kerberos. Nom d'utilisateur utilisé pour la connexion au référentiel. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-RepositoryPassword -rp	repository_password	Obligatoire pour l'authentification native ou LDAP. Facultatif si le domaine utilise l'authentification Kerberos. Mot de passe de l'utilisateur. Vous pouvez définir un mot de passe avec l'option -rp ou la variable d'environnement INFA_REPOSITORY_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -rp est prioritaire.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Obligatoire pour l'authentification LDAP ou l'authentification Kerberos. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel appartient l'utilisateur du référentiel PowerCenter. Le nom du domaine de sécurité est sensible à la casse. Si vous ne spécifiez pas cette option, la commande définit le domaine de sécurité de l'utilisateur du référentiel sur natif.
-FolderName -fn	repository_folder_name	Obligatoire. Nom du dossier contenant la session. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-Workflow -wf	workflow_name	Obligatoire. Nom du flux de travail contenant la session. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-RunInstance -in	run_instance_name	Nom de l'instance d'exécution du flux de travail qui contient la session. Utilisez cette option si vous exécutez des flux de travail simultanés. Utilisez soit l'option -in, soit l'option -id, mais pas les deux.
-RunId -id	workflow_run_id	Identifiant d'exécution de l'instance d'exécution du flux de travail qui contient la session. Utilisez cette option si vous exécutez des flux de travail simultanés. Utilisez soit l'option -in, soit l'option -id, mais pas les deux. Remarque: Utilisez cette option si le flux de travail ne possède pas de nom d'instance d'exécution unique.
-Session -ss	session_name	Obligatoire. Nom de session. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.

GetSystemLogDirectory

Renvoie le chemin du répertoire des journaux système.

Vous devez entrer cette commande sur le domaine pour lequel vous souhaitez obtenir le chemin du répertoire des journaux système.

La commande infacmd isp GetSystemLogDirectory utilise la syntaxe suivante :

```
GetSystemLogDirectory  
[<-OutputFile|-o> output_file]
```

Lorsque vous utilisez la commande sans l'option -o, elle imprime le chemin du répertoire dans la fenêtre de commande. Lorsque vous utilisez l'option -o pour spécifier un fichier de sortie, indiquez le nom et le chemin du fichier de sortie. Par exemple :

```
isp\bin\infacmd.bat getSystemLogDirectory -o c:\sys_log_dir.txt
```

La commande crée un fichier sys_log_dir.txt dans sur le chemin que vous spécifiez et imprime le chemin du répertoire des journaux système dans le fichier. Si le fichier existe, la commande le remplace.

getUserActivityLog

Obtient les journaux d'activité utilisateur pour un ou plusieurs utilisateurs. Vous pouvez écrire les journaux d'activité utilisateur dans un fichier ou les afficher dans la console.

Les données des journaux d'activité utilisateur incluent les tentatives d'ouverture de session réussies et non réussies des clients d'Informatica. Si le client inclut des propriétés personnalisées définies par les clients dans les demandes d'ouverture de session, les données comprennent ces propriétés.

Remarque: Les tentatives d'ouvertures de session ne sont pas capturées dans les journaux d'activité utilisateur dans un domaine configuré pour utiliser l'authentification Kerberos.

La commande infacmd isp getUserActivityLog utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd isp getUserActivityLog` :

Option	Argument	Description
- DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
- SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infra</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
- ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, <code>infacmd</code> utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-Users -usrs	user1:[securitydomain] user2:[securitydomain] ...	<p>Facultatif. Liste des utilisateurs pour lesquels vous souhaitez obtenir les événements du journal. Séparez plusieurs utilisateurs par un espace. Utilisez le symbole de caractère générique (*) pour afficher les journaux de plusieurs utilisateurs sur tous les domaines de sécurité ou un seul d'entre eux. Par exemple, les chaînes suivantes sont les valeurs valides pour cette option :</p> <pre> user:Native "user:*" "user*" "*_users_*" "*:Native" </pre> <p>Si vous utilisez le symbole de caractère générique, placez l'argument entre guillemets.</p> <p>Si vous n'entrez pas d'utilisateur, la commande récupère les événements du journal de tous les utilisateurs.</p>
-StartDate -sd	start_date	<p>Facultatif. Renvoie les événements du journal à partir de la date et de l'heure que vous spécifiez.</p> <p>Entrez la date et l'heure dans l'un des formats suivants :</p> <ul style="list-style-type: none"> - MM/jj/aaaa - MM/jj/aaaa HH:mm:ss - aaaa-MM-jj - aaaa-MM-jj HH:mm:ss
-EndDate -ed	end_date	<p>Facultatif. Renvoie les événements du journal qui se terminent à ces date et heure. Entrez la date et l'heure au même format que l'option StartDate.</p> <p>Si vous entrez une date de fin qui est antérieure à la date de début, la commande ne renvoie aucun événement du journal.</p>
-ActivityCode -ac	activity_code	<p>Facultatif. Renvoie les événements du journal en fonction du code d'activité.</p> <p>Utilisez le symbole de caractère générique (*) pour récupérer les événements du journal pour plusieurs codes d'activité. Les codes d'activité valides sont notamment les suivants :</p> <ul style="list-style-type: none"> - CCM_10437. Indique la réussite d'une activité. - CCM_10438. Indique l'échec d'une activité. - CCM_10778. Indique qu'une tentative de connexion avec des propriétés personnalisées a réussi. - CCM_10779. Indique qu'une tentative de connexion avec des propriétés personnalisées a échoué. - CCM_10786. Indique qu'une tentative de connexion sans propriétés personnalisées a réussi. - CCM_10787. Indique qu'une tentative de connexion sans propriétés personnalisées a échoué.

Option	Argument	Description
-atxt	activity_text	<p>-ActivityText</p> <p>Facultatif. Renvoie les événements du journal en fonction d'une chaîne trouvée dans le texte d'activité.</p> <p>Utilisez le symbole de caractère générique (*) pour récupérer les journaux liés à plusieurs événements. Par exemple, le paramètre suivant renvoie tous les événements du journal qui contiennent « Activation du service » dans leur description :</p> <p>"*Enabling service"</p> <p>Si vous utilisez le symbole de caractère générique, placez l'argument entre guillemets.</p>
- ReverseOrder -ro	True	Facultatif. Imprime les événements du journal dans l'ordre chronologique inverse. Si vous ne spécifiez pas ce paramètre, la commande affiche les événements du journal dans l'ordre chronologique.
-OutputFile -lo	output_file_name	Facultatif. Nom du fichier de sortie. Si vous ne spécifiez pas ce paramètre, la commande affiche le journal sur la ligne de commande.
-Format -fm	output_format_BIN_TEXT_XML	<p>Facultatif. Format du fichier de sortie du journal.</p> <p>Les formats valides sont les suivants :</p> <ul style="list-style-type: none"> - Bin (binaire) - Texte - XML <p>Le format par défaut est le format texte. Si vous spécifiez le format binaire, vous devez indiquer un nom de fichier à l'aide de l'option - OutputFile.</p>

GetWorkflowLog

Obtient les événements du journal pour la dernière exécution d'un flux de travail. Le service de référentiel PowerCenter doit être en cours d'exécution lorsque vous exécutez cette commande.

La commande infacmd isp GetWorkflowLog utilise la syntaxe suivante :

```
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]

```

Remarque: Si vous ne spécifiez pas les options -un, -pd et -sdn, la commande infacmd isp GetWorkflowLog utilise les valeurs correspondantes des options -ru, -rp et -rsdn.

Le tableau suivant décrit les options et arguments d'infacmd isp GetWorkflowLog :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-Format -fm	format	Facultatif. Format du journal de session. Les types valides comprennent : <ul style="list-style-type: none"> - Text - XML - Bin (binaire) Si vous choisissez le format binaire, vous devez spécifier un nom de fichier à l'aide de l'option OutputFile. Si vous ne spécifiez aucun format, <i>infacmd</i> utilise le format texte avec des lignes limitées à 80 caractères.
-OutputFile -lo	output_file_name	Nom et chemin du fichier de journalisation de flux de travail. Par défaut, le gestionnaire de service utilise le répertoire server\infa_shared\log sur le nœud principal de passerelle. Omettez cette option pour afficher les événements du journal à l'écran. Si vous choisissez le type de fichier de sortie binaire, vous devez spécifier un nom de fichier à l'aide de cette option.
-IntegrationService -is	integration_service_name	Obligatoire. Nom du service d'intégration qui exécute le flux de travail. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-RepositoryService -rs	repository_service_name	Obligatoire. Nom du service de référentiel qui contient le flux de travail. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-RepositoryDomain -rd	domain_of_repository	Obligatoire si le référentiel ne se trouve pas dans le domaine local. Domaine du service de référentiel. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.

Option	Argument	Description
-RepositoryUser -ru	user	Obligatoire pour l'authentification native ou LDAP. Facultatif si le domaine utilise l'authentification Kerberos. Nom d'utilisateur utilisé pour la connexion au référentiel. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-RepositoryPassword -rp	mot de passe	Obligatoire pour l'authentification native ou LDAP. Facultatif si le domaine utilise l'authentification Kerberos. Mot de passe de l'utilisateur. Vous pouvez définir un mot de passe avec l'option -rp ou la variable d'environnement INFA_REPOSITORY_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -rp est prioritaire.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Obligatoire pour l'authentification LDAP ou l'authentification Kerberos. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel appartient l'utilisateur du référentiel PowerCenter. Le nom du domaine de sécurité est sensible à la casse. Si vous ne spécifiez pas cette option, la commande définit le domaine de sécurité de l'utilisateur du référentiel sur natif.
-FolderName -fn	repository_folder_name	Obligatoire. Nom du dossier contenant le flux de travail. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-Workflow -wf	workflow_name	Obligatoire. Nom du flux de travail. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-RunInstance -in	run_instance_name	Nom de l'instance d'exécution du flux de travail. Utilisez cette option si vous exécutez des flux de travail simultanés. Utilisez soit l'option -in, soit l'option -id, mais pas les deux.
-RunId -id	workflow_run_id	Identifiant d'exécution de l'instance d'exécution du flux de travail. Utilisez cette option si vous exécutez des flux de travail simultanés. Utilisez soit l'option -in, soit l'option -id, mais pas les deux. Remarque: Utilisez cette option si le flux de travail ne possède pas de nom d'instance d'exécution unique.

Aide

Affiche les options et arguments pour une commande infacmd.

Si vous omettez le nom de commande, infacmd liste toutes les commandes.

La commande infacmd Help utilise la syntaxe suivante :

```
Help <-plugin_ID> [command]
```

Par exemple, si vous saisissez `infacmd isp Help GetServiceStatus`, `infacmd` renvoie les options et les arguments suivants de la commande `infacmd isp GetServiceStatus` :

```
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
```

Le tableau suivant décrit les options et arguments d'`infacmd as Help` :

Option	Argument	Description
-	plugin_ID	Facultatif. Décrit le programme <code>infacmd</code> pour lequel de l'aide sera affichée. La valeur par défaut est <code>isp</code> .
-	command	Facultatif. Nom de commande. Si vous omettez le nom de commande, <code>infacmd</code> liste toutes les commandes.

ImportDomainObjects

Importe des utilisateurs natifs, des groupes natifs, des rôles, des connexions et des configurations de grappe à partir d'un fichier XML dans un domaine Informatica.

Si vous ne souhaitez pas importer tous les objets du fichier, utilisez le fichier de contrôle d'exportation `infacmd` pour filtrer les objets à importer.

Utilisez les commandes `ExportDomainObjects` et `ImportDomainObjects` pour migrer des objets entre deux domaines différents de la même version. Pour importer des utilisateurs et groupes natifs à partir de domaines de versions différentes, utilisez la commande `infacmd isp ImportUsersAndGroups`.

Lorsque vous importez un groupe, vous importez tous les sous-groupes et utilisateurs de ce groupe.

Si la commande échoue et renvoie une erreur de mémoire Java, augmentez la mémoire système disponible pour `infacmd`. Pour augmenter la mémoire système, définissez la valeur `-Xmx` dans la variable d'environnement `ICMD_JAVA_OPTS`.

La commande `infacmd isp ImportDomainObjects` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ImportDomainObjects :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	password	<p>Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p> <p>Pour un compte utilisateur natif, si vous activez la complexité du mot de passe, utilisez les directives suivantes lorsque vous créez ou modifiez un mot de passe :</p> <ul style="list-style-type: none"> - Le mot de passe doit contenir au moins huit caractères. - Il doit être composé d'un caractère alphabétique, d'un caractère numérique et d'un caractère non alphanumérique, tels que : <pre> ! \ " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { } ~ </pre> <p>Lorsque vous utilisez des caractères spéciaux dans un mot de passe, il arrive que l'interpréteur de commandes les lise différemment. Par exemple, \$ est interprété comme une variable. Dans ce cas, utilisez un caractère d'échappement pour échapper le caractère spécial.</p>

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port...	<p>Obligatoire si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.</p>

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ImportFilePath -fp	import_file_path	Obligatoire. Chemin et nom du fichier XML depuis lequel vous importez les objets.
-ImportControlFile -cp	import_control_file	Facultatif. Chemin et nom du fichier de contrôle d'importation qui filtre les objets importés.
-ConflictResolution -cr	resolution_type	<p>Facultatif. Stratégie de résolution de conflit. Vous pouvez spécifier l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> - rename - replace - reuse <p>L'option est ignorée si vous spécifiez une stratégie de résolution de conflit dans le fichier de contrôle d'importation. Si un conflit se produit alors que vous n'avez pas défini de stratégie de résolution de conflit, l'importation échoue.</p> <p>Remarque: Vous ne pouvez pas utiliser l'option rename avec une configuration de cluster.</p> <p>Remarque: La complexité du mot de passe n'est pas obligatoire lorsque vous l'utilisez avec l'option reuse.</p>

ImportUsersAndGroups

Importe des utilisateurs et des groupes natifs dans le domaine.

Exécutez infacmd isp ImportUsersAndGroups pour importer des utilisateurs et des groupes à partir d'un fichier XML.

Si la commande échoue et renvoie une erreur de mémoire Java, augmentez la mémoire système disponible pour infacmd. Pour augmenter la mémoire système, définissez la valeur -Xmx dans la variable d'environnement ICMD_JAVA_OPTS.

La commande infacmd isp ImportUsersAndGroups utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ImportUsersAndGroups :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	password	<p>Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p> <p>Pour un compte utilisateur natif, si vous activez la complexité du mot de passe, utilisez les directives suivantes lorsque vous créez ou modifiez un mot de passe :</p> <ul style="list-style-type: none"> - Le mot de passe doit contenir au moins huit caractères. - Il doit être composé d'un caractère alphabétique, d'un caractère numérique et d'un caractère non alphanumérique, tels que : ! \ " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { } ~ <p>Lorsque vous utilisez des caractères spéciaux dans un mot de passe, il arrive que l'interpréteur de commandes les lise différemment. Par exemple, \$ est interprété comme une variable. Dans ce cas, utilisez un caractère d'échappement pour échapper le caractère spécial.</p>
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port...	<p>Obligatoire si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.</p>

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ExportFile -ef	export_file_name	Obligatoire. Nom et chemin du fichier d'exportation qui contient les informations relatives aux utilisateurs et aux groupes.
-ReuseDomainUsersAndGroups -rd	-	Facultatif. S'il existe un conflit de nom, infacmd conserve les utilisateurs et les groupes définis dans le domaine cible. Par défaut, la commande échoue si elle rencontre un conflit.
-exportedFromPowercenter -epc	-	Obligatoire si le fichier d'exportation a été exporté depuis un domaine d'une version 8.6.1 de PowerCenter.

LIENS CONNEXES :

- ["ExportUsersAndGroups" à la page 544](#)

ListAlertUsers

Répertorie les utilisateurs abonnés à des alertes.

La commande infacmd isp ListAlertUsers utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListAlertUsers :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

listAllCustomLDAPTypes

Répertorie les informations de configuration pour tous les types LDAP personnalisés utilisés par le domaine spécifié.

La commande infacmd isp ListLDAPConnectivity utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd isp listAllCustomLDAPTypes :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

ListAllGroups

Répertorie tous les groupes du domaine de sécurité natif.

La commande infacmd isp ListAllGroups utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListAllGroups :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

listAllLDAPConnectivity

Répertorie les informations de configuration pour toutes les configurations LDAP utilisées par le domaine spécifié.

La commande infacmd isp ListLDAPConnectivity utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd isp listAllLDAPConnectivity :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

ListAllRoles

Répertorie tous les rôles dans le domaine.

La commande infacmd isp ListAllRoles utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListAllRoles :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

ListAllUsers

Répertorie tous les comptes utilisateur dans le domaine.

La commande infacmd isp ListAllUsers utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListAllUsers :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

ListConnectionOptions

Répertorie les options pour une connexion. Exécutez cette commande pour afficher les options disponibles à configurer lorsque vous mettez une connexion à jour.

La commande infacmd isp ListConnectionOptions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListConnectionOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConnectionName -cn	connection_name_security_domain	Obligatoire. Nom de la connexion.

ListConnectionPermissions

Répertorie les autorisations dont un utilisateur ou un groupe dispose pour une connexion.

La commande infacmd isp ListConnectionPermissions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListConnectionPermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-RecipientUserName -run	recipient_user_name	Obligatoire si vous ne spécifiez pas le nom du groupe destinataire. Nom de l'utilisateur dont les autorisations doivent être répertoriées.
-RecipientGroupName -rgn	recipient_group_name	Obligatoire si vous ne spécifiez pas le nom d'utilisateur du destinataire. Nom du groupe dont les autorisations doivent être répertoriées.
-RecipientSecurityDomain -rsd	recipient_security_domain_name	Obligatoire si le destinataire appartient à un domaine de sécurité LDAP. Nom du domaine de sécurité auquel appartient le destinataire. La valeur par défaut est Natif.
-ConnectionName -cn	connection_name_security_domain	Requis. Nom de la connexion.

ListConnectionPermissionsByGroup

Répertorie tous les groupes disposant d'autorisations sur une connexion, de même que le type des autorisations.

La commande infacmd isp ListConnectionPermissionsByGroup utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListConnectionPermissionsByGroup :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConnectionName -cn	connection_name_security_domain	Obligatoire. Nom de la connexion.

ListConnectionPermissionsByUser

Répertorie les utilisateurs disposant d'autorisations pour une connexion, de même que le type des autorisations.

La commande infacmd isp ListConnectionPermissionsByUser utilise la syntaxe suivante :

```
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
```


Le tableau suivant décrit les options et arguments d'infacmd isp ListConnectionPermissionsByUser :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConnectionName -cn	connection_name_security_domain	Obligatoire. Nom de la connexion.

ListConnections

Répertorie les noms de connexion par type. Vous pouvez répertorier par tous les types de connexion ou filtrer les résultats par un type de connexion.

La commande infacmd isp ListConnections utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListConnections :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ConnectionType -ct	connection_type	Facultatif. Vous pouvez filtrer les résultats avec l'option -ct. Utilisez n'importe quel type de connexion pris en charge comme valeur pour l'option -ct. L'entrée n'est pas sensible à la casse. Pour afficher une liste des types de connexion à utiliser avec cette option, exécutez la commande suivante : <code>./infacmd.sh isp listConnections</code> La commande répertorie tous les types de connexion et les connexions que vous avez configurées sur le domaine.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

ListConnectionOptions

Répertorie les options pour une connexion. Exécutez cette commande pour afficher les options disponibles à configurer lorsque vous mettez une connexion à jour.

La commande infacmd isp ListConnectionOptions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListConnectionOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConnectionName -cn	connection_name_security_domain	Obligatoire. Nom de la connexion.

listCustomLDAPType

Répertorie les informations de configuration pour un type LDAP personnalisé.

La commande infacmd isp listCustomLDAPType utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd isp listCustomLDAPType` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-CustomLDAPTypeName -lt	custom_LDAP_type_name	Obligatoire. Nom du type LDAP personnalisé.

ListDefaultOSProfiles

Répertorie les profils de système d'exploitation par défaut pour le groupe ou l'utilisateur donné.

La syntaxe de la commande infacmd isp ListDefaultOSProfiles est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd isp ListDefaultOSProfiles :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine.
-RecipientName -nm	recipient_name	Facultatif. Nom d'utilisateur ou nom de groupe auquel attribuer le profil de système d'exploitation par défaut.
-RecipientSecurityDomain -ns	security_domain_of_recipient	Facultatif. Nom du domaine de sécurité auquel l'utilisateur appartient, si vous utilisez l'authentification LDAP.
-RecipientType -ty	recipient_type	Facultatif. Indiquez si le destinataire est un utilisateur ou un groupe. Entrez l'une des valeurs suivantes : - Useridentity - Groupidentity
-IndirectInheritance -in	indirect_inheritance	Facultatif. Entrez l'une des valeurs suivantes : - True. Répertorie les profils de système d'exploitation dont les utilisateurs ou les groupes héritent. - False. Répertorie les profils de système d'exploitation directement attribués aux utilisateurs ou aux groupes.

ListDomainCiphers

Répertorie une ou plusieurs des listes de suites de chiffres suivantes : liste noire, liste par défaut, liste effective ou liste blanche.

Lorsque vous utilisez la communication sécurisée dans le domaine et des connexions sécurisées pour les clients Web, Informatica utilise une liste de suites de chiffres effective pour crypter le trafic. Informatica détermine la liste de suites de chiffres effective en fonction des listes suivantes :

Liste noire

Liste de suites de chiffres que vous souhaitez voir bloquées par le domaine Informatica. Lorsque vous ajoutez une suite de chiffres à la liste noire, le domaine Informatica la supprime de la liste effective. Vous pouvez ajouter à la liste noire des suites de chiffres se trouvant dans la liste par défaut.

Liste par défaut

Liste de suites de chiffres prises en charge par défaut par le domaine Informatica.

Liste blanche

Liste de suites de chiffres que vous voulez voir prises en charge par le domaine Informatica en plus de la liste par défaut. Lorsque vous ajoutez une suite de chiffres à la liste blanche, le domaine Informatica l'ajoute à la liste effective. Il n'est pas nécessaire d'ajouter les suites de chiffres de la liste par défaut à la liste blanche.

Utilisez la commande ListDomainCiphers pour afficher les listes de suites de chiffres.

La commande infacmd isp ListDomainCiphers utilise la syntaxe suivante :

```
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)]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListDomainCiphers :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
- SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-lists -l	comma_separated_list_of_cipher_configurations	<p>Facultatif. Liste d'arguments séparés par des virgules qui spécifie les suites de chiffrement à afficher.</p> <p>L'argument ALL affiche la liste noire, la liste par défaut, la liste effective et la liste blanche.</p> <p>L'argument BLACK affiche la liste noire.</p> <p>L'argument DEFAULT affiche la liste par défaut.</p> <p>L'argument EFFECTIVE affiche la liste des suites de chiffrement pris en charge par le domaine Informatica.</p> <p>L'argument WHITE affiche la liste blanche.</p> <p>Remarque: Les arguments sont sensibles à la casse.</p> <p>Lorsque vous exécutez la commande sur un nœud de passerelle et omettez cette option, la commande affiche toutes les listes de suites de chiffres.</p> <p>Lorsque vous exécutez la commande sur un nœud de travail et omettez cette option, la commande affiche les listes de suites de chiffres effective et par défaut.</p>

ListDomainLinks

Répertorie les domaines auxquels le domaine local peut se connecter. Etablissez des liens entre deux domaines si vous souhaitez échanger des métadonnées du référentiel entre eux.

La commande infacmd isp ListDomainLinks utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListDomainLinks :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine local.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine local. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

ListDomainOptions

Répertorie les propriétés générales du domaine. Les propriétés incluent le dépassement de délai de résilience, la limite des dépassement de délai de résilience, le nombre maximal de tentatives de redémarrage, la période de redémarrage, le mode SSL et le mode de répartition.

Pour exécuter la commande infacmd isp ListDomainOptions, vous devez avoir l'autorisation sur le domaine.

La commande infacmd isp ListDomainOptions utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListDomainOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

ListFolders

Répertorie les dossiers dans le domaine.

La commande infacmd isp ListFolders utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListFolders :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

ListGridNodes

Répertorie les nœuds assignés à une grille.

Pour exécuter la commande infacmd isp ListGridNodes, vous devez avoir l'autorisation sur la grille.

La commande infacmd isp ListGridNodes utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'*infacmd isp ListGridNodes* :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-GridName -gn	grid_name	Obligatoire. Nom de la grille.

ListGroupPermissions

Répertorie les autorisations du groupe sur un objet.

La commande infacmd isp ListGroupPermissions utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListGroupPermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ExistingGroup -eg	existing_group_name	Obligatoire. Nom du groupe auquel vous souhaitez attribuer une autorisation sur un objet.
-ExistingGroupSecurityDomain -egn	existing_group_security_domain_name	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité du groupe auquel vous souhaitez attribuer une autorisation. La valeur par défaut est Natif.
-ObjectType -ot	object_type	<p>Obligatoire. Type d'objet que vous souhaitez répertorier :</p> <ul style="list-style-type: none"> - Service - Licence - Nœud - Grille - Dossier - OSProfile

ListGroupPrivileges

Répertorie les privilèges assignés à un groupe dans le domaine. Vous pouvez répertorier des privilèges de groupes pour chaque application dans le domaine.

La commande infacmd isp ListGroupPrivileges utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListGroupPrivileges :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-GroupName -gn	group_name	Obligatoire. Nom du groupe dont vous souhaitez répertorier les privilèges.
-GroupSecurityDomain -gsf	group_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient le groupe dont vous souhaitez répertorier les privilèges. La valeur par défaut est Natif.
-ServiceName -sn	service_name	Obligatoire. Nom de service du domaine ou de l'application dont vous souhaitez afficher les privilèges.

ListGroupsForUser

Répertorie les groupes natifs auxquels l'utilisateur est affecté.

La commande infacmd isp ListGroupsForUser utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListGroupsForUser :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ExistingUserName -eu	existing_user_Name	Requis. Nom de l'utilisateur dont vous souhaitez répertorier les groupes.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. La valeur par défaut est Natif.

ListLDAPConnectivity

Répertorie les détails de la configuration LDAP spécifiée.

La commande infacmd isp ListLDAPConnectivity utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListLDAPConnectivity :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-LDAPHostConfigurationName -lcn	LDAP_host_configuration_name	Obligatoire. Nom de la configuration LDAP.

ListLicenses

Répertorie les licences dans le domaine. Vous pouvez afficher le nom de licence et le numéro de série pour chaque licence.

Pour exécuter la commande infacmd isp ListLicenses, vous devez avoir l'autorisation sur les licences.

La commande infacmd isp ListLicenses utilise la syntaxe suivante :

```
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]
```


Le tableau suivant décrit les options et arguments d'infacmd isp ListLicenses :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

ListMonitoringOptions

Répertoriez les propriétés générales de surveillance.

La commande infacmd isp listMonitoringOptions utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd isp listMonitoringOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel la commande infacmd tente d'établir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire. La valeur par défaut est 180 secondes.

ListNodeOptions

Répertorie les propriétés générales pour un nœud. Les propriétés générales incluent le répertoire de sauvegarde, le profil du processeur, le niveau de gravité d'erreur, les ports de processus maximaux et minimaux, ainsi que les seuils de fourniture de ressources.

Pour exécuter la commande infacmd isp ListNodeOptions, vous devez avoir l'autorisation sur le nœud.

La commande infacmd isp ListNodeOptions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListNodeOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NodeName -nn	node_name	Obligatoire. Nom du nœud dont vous souhaitez répertorier les options.

ListNodeResources

Répertorie toutes les ressources définies pour un nœud. Pour chaque ressource, cette commande renvoie son type et son état de disponibilité.

Pour exécuter la commande infacmd isp ListNodeResources, vous devez avoir l'autorisation sur le nœud.

La commande infacmd isp ListNodeResources utilise la syntaxe suivante :

```
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")]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListNodeResources :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NodeName -nn	node_name	Requis. Nom du nœud dont vous souhaitez répertorier les ressources.
-ResourceCategory -rc	resource_category	Facultatif. Catégorie des ressources à répertorier. Les catégories valides comprennent : <ul style="list-style-type: none"> - PCIS. Ressource pour le service d'intégration PowerCenter. - DIS. Réserve pour un usage futur. La valeur par défaut est PCIS.

ListNodeRoles

Répertorie tous les rôles sur un nœud du domaine.

La commande infacmd isp ListNodeRoles utilise la syntaxe suivante :

```
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

Le tableau suivant décrit les options et les arguments de la commande infacmd isp ListNodeRoles :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NodeName -nn	node_name	Requis. Nom du nœud.

ListNodes

Répertorie les nœuds dans le domaine. Si vous n'utilisez pas l'option de rôle de nœud, la commande répertorie tous les nœuds dans le domaine. Si vous utilisez l'option de rôle de nœud, la commande répertorie les nœuds avec le rôle spécifié.

La commande infacmd isp ListNodes utilise la syntaxe suivante :

```
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]
```


Le tableau suivant décrit les options et arguments d'infacmd isp ListNodes :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NodeRole -nr	node_role	Facultatif. Rôle activé sur les nœuds à répertorier. Entrez l'une des valeurs suivantes : <ul style="list-style-type: none"> - Service. Répertorie les nœuds contenant au moins le rôle de service. - Compute. Répertorie les nœuds contenant au moins le rôle de calcul. - Service_compute. Répertorie les nœuds contenant les rôles de service et de calcul. Si vous omettez cette option, la commande répertorie tous les nœuds du domaine.

ListOSProfiles

Répertorie les profils du système d'exploitation dans le domaine.

La commande infacmd isp ListOSProfile utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListOSProfile :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

ListRepositoryLDAPConfiguration

Répertorie les options de configuration du serveur LDAP telles que l'adresse du serveur LDAP, le domaine de recherche et les attributs de connexion.

Utilisez cette commande après avoir installé Informatica pour vérifier la connexion entre le domaine et le service de répertoire externe LDAP.

Utilisez `infacmd isp SetRepositoryLDAPConfiguration` pour mettre à jour les options de configuration du serveur LDAP pour un domaine Informatica. Vous utilisez cette commande lorsque vous mettez à niveau un référentiel qui utilise d'authentification LDAP.

La commande `infacmd isp ListRepositoryLDAPConfiguration` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'`infacmd isp ListRepositoryLDAPConfiguration` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

ListRolePrivileges

Répertorie les privilèges assignés à un rôle dans le domaine. Vous pouvez répertorier des privilèges de rôles pour chaque service d'application dans le domaine.

Vous pouvez lister les privilèges affectés à un rôle pour le domaine et pour chaque type de service d'application dans le domaine.

La commande infacmd isp ListRolePrivileges utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments de ListRolePrivileges :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-RoleName -rn	role_name	Obligatoire. Nom du rôle dont vous souhaitez répertorier les privilèges. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.

ListSecurityDomains

Répertorie les domaines de sécurité natif et LDAP dans le domaine.

La commande infacmd isp ListSecurityDomains utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListSecurityDomains :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

ListServiceLevels

Répertorie les niveaux de services définis pour le domaine. Vous pouvez répertorier le nom, la priorité de répartition et le temps d'attente de répartition maximal pour chaque niveau de service.

La commande infacmd isp ListServiceLevels utilise la syntaxe suivante :

```
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]
```


Le tableau suivant décrit les options et arguments d'infacmd isp ListServiceLevels :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

ListServiceNodes

Répertorie la grille ou les nœuds assignés à un service.

Si cette commande renvoie un nom de grille, vous pouvez exécuter la commande `infacmd isp ListGridNodes` pour répertorier les nœuds de la grille.

Pour exécuter la commande `infacmd isp ListServiceNodes`, vous devez avoir l'autorisation sur le service.

La commande `infacmd isp ListServiceNodes` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'`infacmd isp ListServiceNodes` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Obligatoire. Nom du service.

LIENS CONNEXES :

- [“ListGridNodes” à la page 611](#)

ListServicePrivileges

Répertorie les privilèges pour un domaine ou un type de service d'application.

La commande infacmd isp ListServicePrivileges utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListServicePrivileges :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceType -st	service_type	Facultatif. Type de service de domaine ou d'application dont vous voulez afficher les privilèges. Les types de services comprennent : <ul style="list-style-type: none"> - AS. Service Analyst - CMS. Service de gestion de contenu - CS. Service de catalogue - MM. Service Metadata Manager - MRS. Service de référentiel modèle - RS. Service de référentiel PowerCenter - TDM. Service Test Data Manager - TDW. Service Test Data Warehouse - DOMAIN. Domaine

ListServices

Répertorie les services dans le domaine.

La commande infacmd isp ListServices utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListServices :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_se conds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceType -st	service_type	Facultatif. Répertorie tous les services d'un type spécifique. Les types de services comprennent : <ul style="list-style-type: none"> - AS. Service Analyst - BW. Service SAP BW - CMS. Service de gestion de contenu - DIS. Service d'intégration de données - ES. Service de messagerie électronique - IHS. Service de grappe Informatica - IS. Service d'intégration PowerCenter - CS. Service de catalogue - MM. Service Metadata Manager - MRS. Service de référentiel modèle - RMS. Service de gestionnaire de ressource - RS. Service de référentiel PowerCenter - SCH. Service de planificateur - SEARCH. Service de recherche - TDM. Service Test Data Manager - TDW. Service Test Data Warehouse - WS. Hub des services Web

ListSMTPOptions

Répertorie les propriétés de configuration SMTP du domaine. La configuration SMTP est utilisée pour envoyer des alertes de domaine et des notifications de fiche d'évaluation.

La commande infacmd isp ListSMTPOptions utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListSMTPOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

LIENS CONNEXES :

- [“UpdateSMTPOptions” à la page 784](#)

ListUserPermissions

Répertorie les objets de domaines sur lesquels un utilisateur dispose d'autorisations.

La commande infacmd isp ListUserPermissions utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListUserPermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ExistingUserName -eu	existing_user_name	Obligatoire. Compte utilisateur dont vous souhaitez répertorier les privilèges. Pour saisir un nom qui contient des espaces ou d'autres caractères non alphanumériques, placez-le entre guillemets.

Option	Argument	Description
-ExistingUserSecurityDomain -esd	existing_user_security_do mainth_name	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur dont vous souhaitez répertorier les privilèges. La valeur par défaut est Natif.
-ObjectType -ot	object_type	Obligatoire. Type d'objet que vous souhaitez répertorier : <ul style="list-style-type: none"> - Service - Licence - Nœud - Grille - Dossier - OSProfile

ListUserPrivileges

Répertorie les privilèges assignés à un utilisateur dans le domaine. Vous pouvez répertorier des privilèges d'utilisateurs pour chaque service d'application dans le domaine.

La commande infacmd isp ListUserPrivileges utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp ListUserPrivileges :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
ExistingUserName -eu	existing_user_name	Obligatoire. Compte utilisateur dont vous souhaitez répertorier les privilèges. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur dont vous souhaitez répertorier les privilèges. La valeur par défaut est Natif.
-ServiceName -sn	service_name	Obligatoire. Nom de service du domaine ou de l'application dont vous souhaitez afficher les privilèges.

infacmd ListWeakPasswordUsers

Répertorie les utilisateurs avec des mots de passe qui ne répondent pas à la stratégie de mot de passe.

La syntaxe de la commande infacmd ListWeakPasswordUsers est la suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd ListWeakPasswordUsers :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.

Option	Argument	Description
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Spécifiez les noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire. La valeur par défaut est 180 secondes.

migrateUsers

Migre les groupes, les rôles, les privilèges et les autorisations des utilisateurs du domaine de sécurité natif vers des utilisateurs d'un ou plusieurs domaines de sécurité LDAP. Avant de configurer un domaine pour utiliser l'authentification Kerberos, vous devez migrer les utilisateurs vers un domaine de sécurité LDAP.

Pour plus d'informations sur la commande migrateUsers, consultez le *Guide de sécurité Informatica*.

La commande infacmd isp migrateUsers utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd isp migrateUsers` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	administrator_user_name	Obligatoire. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Password -pd	administrator_password	Obligatoire. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Facultatif. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Remarque: Ce domaine de sécurité est le domaine de sécurité du compte utilisateur utilisé pour se connecter au domaine, pas le domaine de sécurité vers lesquels les utilisateurs doivent être migrés.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Facultatif. À utiliser si les informations de connectivité de passerelle dans le fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-UserMigrationFile -umf	user_migration_file	<p>Obligatoire. Chemin et nom du fichier de migration d'utilisateur. Le fichier de migration d'utilisateur est un fichier texte qui contient la liste des utilisateurs natifs et des utilisateurs LDAP correspondants. Les entrées doivent être au format suivant :</p> <p>Native/<SourceUserName>,LDAP/<TargetUsername></p> <p>Par exemple, pour migrer un utilisateur nommé user1 du domaine de sécurité natif vers un utilisateur nommé User1 d'un domaine de sécurité LDAP, ajoutez la ligne suivante au fichier de migration d'utilisateur :</p> <p>Native/User1,LDAP/User1</p> <p>La commande ignore les entrées comportant un nom d'utilisateur source ou un nom d'utilisateur cible en double.</p>

MoveFolder

Déplace un dossier.

La commande infacmd isp MoveFolder utilise la syntaxe suivante :

```
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
```


Le tableau suivant décrit les options et arguments d'infacmd isp MoveFolder :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-OriginalPath -op	original_folder_path	Obligatoire. Chemin d'accès complet, sans le nom de domaine, du dossier que vous souhaitez déplacer. Doit être au format suivant : <i>/parent_folder/child_folder</i>
-FolderPath -fp	full_folder_path	Obligatoire. Chemin d'accès complet, sans le nom de domaine, du dossier cible. Doit être au format suivant : <i>/parent_folder/child_folder</i>

MoveObject

Déplace un objet vers un autre dossier.

La commande infacmd isp MoveObject utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp MoveObject :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ObjectName -on	object_name	Obligatoire. Nom de l'objet que vous souhaitez déplacer.

Option	Argument	Description
-ObjectType -ot	object_type	Obligatoire. Type d'objet que vous souhaitez déplacer : <ul style="list-style-type: none"> - Service - Licence - Nœud - Grille
-FolderPath -fp	full_folder_path	Obligatoire. Chemin d'accès complet, sans le nom de domaine, du dossier vers lequel vous souhaitez déplacer l'objet. Doit être au format suivant : <i>/parent_folder/child_folder</i>

Ping

Envoie une commande ping à un domaine, un service, un hôte de passerelle du domaine ou encore un nœud. Si l'objet est disponible, cette commande affiche un message spécifiant qu'il est disponible au niveau d'un port spécifique de la machine de l'hôte de passerelle. Si l'objet est indisponible, cette commande affiche un message indiquant qu'il n'a pas pu recevoir de réponse de la part de l'objet.

Utilisez cette commande pour résoudre les connexions réseau. Pour exécuter la commande `infacmd isp Ping`, vous devez avoir l'autorisation sur l'objet sur lequel vous voulez faire un ping.

La commande `infacmd isp Ping` n'affiche pas les résultats des processus de service individuels.

La commande `infacmd isp Ping` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'`infacmd isp Ping` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option <code>-dn</code> ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option <code>-dn</code> est prioritaire.
-ServiceName -sn	service_name	Facultatif. Nom du service sur lequel vous voulez faire un ping. Pour saisir un nom contenant une espace ou tout autre caractère non alphanumérique, placez-le entre guillemets.

Option	Argument	Description
-GatewayAddress -dg	domain_gateway_host:port	Requis si vous ne spécifiez pas l'option -DomainName ou si vous devez faire un ping sur un autre domaine. Nom de machine et numéro de port de l'hôte de passerelle.
-NodeName -nn	node_name	Facultatif. Nom du nœud.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

PingDomain

Effectue un ping sur tous les nœuds et les services d'un domaine. Affiche le statut du domaine, des nœuds et des services. Vous pouvez choisir d'enregistrer la sortie dans un fichier texte ou .csv.

La sortie utilise les formats suivants pour afficher le statut du domaine, des nœuds et des services:

- Domaine. MASTER_NODE_NAME, STATUS, HOST:PORT.
- Nœud. DOMAIN_NAME, NODE_NAME, STATUS, HOST:PORT.
- Service. SERVICE_NAME, NODE_NAME, STATUS, HOST:PORT.

Si un service est désactivé dans le domaine, le statut indique DISABLED. La sortie n'indique pas le nom du nœud, le nom d'hôte et le numéro de port.

Si le service s'exécute sur une grille, la commande effectue un ping sur chaque nœud de la grille. La sortie indique le statut du service sur chaque nœud.

La syntaxe de la commande infacmd isp PingDomain est la suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp PingDomain :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-Format -fm	format_TEXT_CSV	Facultatif. Format d'affichage du statut du domaine, des nœuds et des services. Vous pouvez spécifier TEXT ou CSV. Le format par défaut est TEXT.
-OutputFile -of	output_file_name	Nom et chemin de fichier où vous souhaitez enregistrer le fichier de sortie.

PrintSPNAndKeytabNames

Génère la liste des noms de fichier SPN et Keytab pour les nœuds et les services du domaine. Le domaine Informatica requiert un fichier Keytab pour chaque SPN. Il peut s'avérer nécessaire de demander à l'administrateur Kerberos d'ajouter les SPN à la base de données de principaux et de créer les fichiers Keytab. Les noms de fichier SPN et Keytab sont sensibles à la casse.

La commande `infacmd isp PrintSPNAndKeytabNames` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd isp PrintSPNAndKeytabNames` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceRealmName -srn	realm_name_of_node_spn	Obligatoire. Nom du domaine Kerberos auquel les services du domaine Informatica appartiennent. Le nom du domaine doit être en majuscules et est sensible à la casse.
-Format -fm	format_TEXT_CSV	Facultatif. Format de fichier de sortie. Les types valides comprennent : <ul style="list-style-type: none"> - Text - CSV Si vous ne spécifiez aucun format, <code>infacmd</code> utilise le format texte avec des lignes limitées à 80 caractères.

Option	Argument	Description
-OutputFile -of	output_file_name	Facultatif. Nom et chemin du fichier pour le fichier de sortie. Si vous ne spécifiez pas un nom de fichier de sortie, infacmd affiche les événements du journal sur l'écran.
-DomainNodes -dns	NodeName:HostName [NodeName:Hostna me]	Nom du nœud et nom d'hôte complet de la machine qui héberge le nœud. Utilisez le format suivant : NodeName:HostName Vous pouvez générer des SPN et des noms de fichiers Keytab pour plusieurs nœuds. Séparez chaque paire de noms de nœud et de noms d'hôte par un espace.
-ServiceProcesses -sps	ServiceName:Nodena me [ServiceName:Nodena me]	Facultatif. Nom du service que vous voulez créer dans le domaine Informatica et nom du nœud sur lequel le service sera exécuté. Utilisez le format suivant : ServiceName:NodeName Vous pouvez générer des SPN et des noms de fichiers Keytab pour plusieurs services. Séparez chaque paire de noms de service et de noms de nœud par un espace. Remarque : les fichiers Keytab des services d'application dans le domaine n'ont pas besoin d'être disponibles lorsque vous configurez le domaine pour utiliser l'authentification Kerberos. Vous pouvez ajouter le SPN du service à la base de données de principaux et créer le fichier Keytab après avoir modifié l'authentification du domaine Informatica, mais avant d'activer le service.
SPNShareLevel -spnSL	SPNShareLevel PROCESS NODE]	Facultatif. Indique le niveau du principal du service du domaine. Définissez la propriété sur l'un des niveaux suivants : <ul style="list-style-type: none"> - Processus. Le domaine requiert un nom unique de principal du service (SPN) et un fichier Keytab pour chaque nœud et chaque service sur ce nœud. Le nombre de SPN et de fichiers Keytab requis pour chaque nœud dépend du nombre de processus de service exécutés sur le nœud. Recommandé pour les domaines de production. - Nœud. Le domaine utilise un SPN et un fichier Keytab pour le nœud et tous les services exécutés sur celui-ci. Il requiert également un SPN et un fichier Keytab distincts pour tous les processus HTTP sur le nœud. Recommandé pour les domaines de test et de développement. Recommandé pour les domaines de test et de développement. La valeur par défaut est le processus.

PurgeLog

Purge les événements du journal. Vous pouvez purger les événements du journal pour un domaine ou pour des services d'applications, comme le service d'intégration PowerCenter, le service d'intégration de données et le service Hub des services Web.

La commande infacmd isp PurgeLog utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et arguments d'infacmd isp PurgeLog :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-BeforeDate -bd	before_date	Requis. Purge les événements du journal qui se sont produits avant cette date et heure. Entrez la date et l'heure dans l'un des formats suivants : - MM/dd/yyyy - yyyy-MM-dd

PurgeMonitoringData

Purge les données de surveillance depuis le référentiel modèle.

La commande `purgeMonitoringData` utilise la syntaxe suivante :

```
<-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]
```

Le tableau suivant décrit les options et les arguments de la commande `PurgeMonitoringData` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité de l'utilisateur. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel la commande infacmd tente d'établir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire. La valeur par défaut est 180 secondes.
-NumDaysToRetain -ndr	num_days_to_retain	Facultatif. Nombre de jours pendant lesquels le référentiel modèle conserve les données moyennes. Par exemple, si vous entrez 180, le service de référentiel modèle purge toutes les données moyennes qui ont plus de 180 jours. La valeur minimale est 0. La valeur maximale est 366. Par défaut, l'option -ndr utilise la valeur Conserver le résumé des données de l'historique depuis la configuration de la surveillance.
-NumDaysToRetainDetailedStat -ndrds	num_days_to_retain_detailed_stat	Facultatif. Nombre de jours pendant lesquels le référentiel modèle conserve les données par minute. Par exemple, si vous entrez 7, le service de référentiel modèle purge toutes les données moyennes qui ont plus de 7 jours. La valeur minimale est 0. La valeur maximale est 14. Par défaut, l'option -ndrds utilise la valeur Conserver les données de l'historique détaillé depuis la configuration de la surveillance.

RemoveAlertUser

Désabonne un utilisateur de courriels de notifications d'alertes. Vous pouvez exécuter infacmd isp RemoveAlertUser pour un utilisateur.

La commande infacmd isp RemoveAlertUser utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RemoveAlertUser :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-AlertUser -au	user_name	Obligatoire. Nom de l'utilisateur que vous souhaitez désabonner des alertes.

RemoveConnection

Supprime une connexion du domaine.

La commande infacmd isp RemoveConnection utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RemoveConnection :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConnectionName -cn	connection_name	Nom de la connexion à supprimer.

RemoveConnectionPermissions

Supprime des autorisations de connexion pour un utilisateur ou un groupe.

La commande infacmd isp RemoveConnectionPermissions utilise la syntaxe suivante :

```
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
```


Le tableau suivant décrit les options et arguments d'infacmd isp RemoveConnectionPermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-RecipientUserName -run	recipient_user_name	Obligatoire si vous ne spécifiez pas le nom du groupe destinataire. Nom de l'utilisateur dont les autorisations doivent être supprimées.
-RecipientGroupName -rgn	recipient_group_name	Obligatoire si vous ne spécifiez pas le nom d'utilisateur du destinataire. Nom du groupe dont les autorisations sur la connexion doivent être supprimées.
-RecipientSecurityDomain -rsd	recipient_security_domain_name	Obligatoire si le destinataire appartient à un domaine de sécurité LDAP. Nom du domaine de sécurité auquel appartient le destinataire. La valeur par défaut est Natif.
-ConnectionName -cn	connection_name_security_domain	Requis. Nom de la connexion.

removeCustomLDAPType

Supprime le type LDAP personnalisé spécifié.

La commande infacmd isp removeCustomLDAPType utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments d'infacmd isp removeCustomLDAPType :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-CustomLDAPTypeName -lt	custom_LDAP_type_name	Obligatoire. Nom du type LDAP personnalisé à supprimer.

RemoveDomainLink

Supprime un domaine lié. Lorsque vous supprimez un domaine lié, vous ne pouvez pas échanger de métadonnées du référentiel entre le domaine local et le domaine lié. Il se peut que vous souhaitiez le faire si vous n'avez plus besoin d'accéder à un service de référentiel PowerCenter dans un autre domaine.

La commande infacmd isp RemoveDomainLink utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RemoveDomainLink :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine local.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine local. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-LinkedDomainName -ld	linked_domain_name	Obligatoire. Nom du domaine dont vous souhaitez supprimer une connexion.

RemoveFolder

Supprime un dossier du domaine. Avant de supprimer un dossier, assurez-vous qu'il est vide.

Le dossier doit être vide.

La commande infacmd isp RemoveFolder utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RemoveFolder :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-FolderPath -fp	full_folder_path	Obligatoire. Chemin d'accès complet, sans le nom de domaine, du dossier que vous souhaitez supprimer. Doit être au format suivant : <i>/parent_folder/child_folder</i>

RemoveGrid

Supprime une grille du domaine. Avant de pouvoir retirer une grille, vous devez annuler l'assignation de la grille du service d'intégration PowerCenter ou du service d'intégration de données.

La commande infacmd isp RemoveGrid utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RemoveGrid :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Mot de passe -pd	mot de passe	Obligatoire. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-GridName -gn	grid_name	Obligatoire. Nom de la grille que vous souhaitez supprimer.

RemoveGroup

Supprime un groupe du domaine de sécurité natif.

La commande infacmd isp RemoveGroup utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RemoveGroup :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-GroupName -gn	group_name	Obligatoire. Nom du groupe que vous souhaitez supprimer.

RemoveGroupPermission

Retire une autorisation de groupe à un objet.

La commande infacmd isp RemoveGroupPermission utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RemoveGroupPermission :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ExistingGroup -eg	existing_group_name	Obligatoire. Nom du groupe auquel vous souhaitez attribuer une autorisation sur un objet.
-GroupSecurityDomain -gsf	group_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité du groupe auquel vous souhaitez attribuer une autorisation. La valeur par défaut est Natif.
-ObjectName -on	object_name	Nom de l'objet pour lequel vous souhaitez supprimer l'autorisation d'accès de groupe.
-ObjectType -ot	object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE	Obligatoire. Type d'objet. Entrez l'une des valeurs suivantes : <ul style="list-style-type: none"> - Service - Licence - Nœud - Grille - Dossier - OSProfile

RemoveGroupPrivilege

Retire un privilège d'un groupe dans le domaine. Vous pouvez supprimer un privilège d'un groupe pour le domaine ou un service d'application dans le domaine.

La commande infacmd isp RemoveGroupPrivilege utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RemoveGroupPrivilege :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-GroupName -gn	group_name	Obligatoire. Nom du groupe dont vous supprimez le privilège. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-GroupSecurityDomain -gsf	group_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient le groupe dont vous supprimez des privilèges. La valeur par défaut est Natif.
-ServiceName -sn	service_name	Obligatoire. Nom de service du domaine ou de l'application dont vous souhaitez afficher les privilèges.
-PrivilegePath -pp	path_of_privilege	Obligatoire. Nom complet du privilège que vous souhaitez attribuer au groupe. Un nom complet inclut le nom du groupe de privilèges et le nom du privilège. folder/create constitue par exemple un nom complet de privilège pour le service de référentiel. Si le nom du privilège comprend des espaces, placez le chemin entre guillemets comme suit : "Runtime Objects/Monitor/Execute/Manage Execution" Si le nom du privilège inclut le caractère spécial « / », faites-le précéder du caractère d'échappement « \ », comme suit : "Model/View Model/Export\Import Models"

removeLDAPConnectivity

Supprime la configuration LDAP spécifiée.

La commande infacmd isp removeLDAPConnectivity utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments d'infacmd isp removeLDAPConnectivity :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-LDAPHostConfigurationName -lcn	LDAP_host_configuration_name	Obligatoire. Nom de la configuration LDAP à supprimer.

RemoveLicense

Supprime une licence du domaine. Avant d'exécuter cette commande, vous devez désactiver les services assignés à la licence.

Retire une licence depuis un domaine quand il expire ou lorsque vous voulez déplacer la licence à un autre domaine.

La commande infacmd isp RemoveLicense utilise la syntaxe suivante :

```
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
```


Le tableau suivant décrit les options et arguments d'infacmd isp RemoveLicense :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-LicenseName -ln	license_name	Obligatoire. Nom de la licence à supprimer.

LIENS CONNEXES :

- [“DisableService” à la page 525](#)
- [“UnassignLicense” à la page 728](#)

RemoveNode

Supprime un nœud du domaine. Si le nœud s'exécute, vous devez d'abord le fermer.

La commande infacmd isp RemoveNode utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RemoveNode :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NodeName -nn	node_name	Obligatoire. Nom du nœud que vous souhaitez supprimer.

RemoveNodeResource

Supprime une ressource d'un nœud. Vous pouvez supprimer un fichier, un répertoire ou une ressource personnalisée d'un nœud. Vous ne pouvez pas supprimer de ressource de connexion d'un nœud.

Quand un service d'intégration PowerCenter est exécuté sur une grille, l'équilibrage de charge peut utiliser des ressources pour distribuer des tâches Session, Command et Event-wait prédéfinies. Si le service d'intégration PowerCenter est configuré pour vérifier des ressources, l'équilibrage de charge distribue des tâches aux nœuds où les ressources sont ajoutées et activées. Si vous supprimez une ressource qui est requise par la tâche Session ou Command, la tâche ne peut plus être exécutée sur ce nœud.

La commande infacmd isp RemoveNodeResource utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RemoveNodeResource :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NodeName -nn	node_name	Requis. Nom du nœud comportant la ressource que vous souhaitez supprimer.
-ResourceCategory -rc	resource_category	Facultatif. Catégorie de ressource à supprimer. Les catégories valides comprennent : - PCIS. Ressource pour le service d'intégration PowerCenter. - DIS. Réserve pour un usage futur. La valeur par défaut est PCIS.
-ResourceType -rt	resource_type	Requis. Type de ressource que vous souhaitez supprimer. Les types valides comprennent : - Personnalisé - Répertoire de fichier
-ResourceName -rn	resource_name	Requis. Nom complet de la ressource que vous souhaitez supprimer. Pour répertorier les noms de toutes les ressources disponibles pour un nœud, exécutez la commande infacmd isp ListNodeResources.

RemoveOSProfile

Supprime un profil du système d'exploitation du domaine.

La commande infacmd isp RemoveOSProfile utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RemoveOSProfile :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-OSProfileName -on	OSProfile_name	Obligatoire. Nom du profil de système d'exploitation que vous souhaitez supprimer.

RemoveRole

Supprime un rôle personnalisé du domaine. Lorsque vous supprimez un rôle personnalisé, ce dernier et tous les privilèges qu'il contenait sont supprimés de tous les utilisateurs ou groupes assignés au rôle.

La commande infacmd isp RemoveRole utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RemoveRole :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-RoleName -rn	role_name	Obligatoire. Nom du rôle que vous souhaitez supprimer.

RemoveRolePrivilege

Supprime un privilège d'un rôle du domaine ou d'un rôle d'un service d'application dans le domaine.

La commande infacmd isp RemoveRolePrivilege utilise la syntaxe suivante :

```
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
```


Le tableau suivant décrit les options et arguments d'infacmd isp RemoveRolePrivilege :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-RoleName -rn	role_name	Requis. Nom du rôle dont vous supprimez le privilège. Pour entrer un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-ServiceType -st	service_type	Requis. Type de service de domaine ou d'application dont vous souhaitez supprimer le privilège pour le rôle. Les types de services comprennent : <ul style="list-style-type: none"> - AS. Service Analyst - CMS. Service de gestion de contenu - CS. Service de catalogue - MM. Service Metadata Manager - MRS. Service de référentiel modèle - RS. Service de référentiel PowerCenter - TDM. Service Test Data Manager - TDW. Service Test Data Warehouse - DOMAIN. Domaine
-PrivilegePath -pp>	path_of_privilege	Requis. Nom complet du privilège que vous souhaitez attribuer au groupe. Un nom complet inclut le nom du groupe de privilèges et le nom du privilège. folder/create constitue par exemple un nom complet de privilège pour le service de référentiel. Si le nom du privilège comprend des espaces, placez le chemin entre guillemets comme suit : "Runtime Objects/Monitor/Execute/Manage Execution" Si le nom du privilège inclut le caractère spécial « / », faites-le précéder du caractère d'échappement « \ », comme suit : "Model/View Model/Export\Import Models"

RemoveService

Supprime un service d'application du domaine. Avant de supprimer un service, vous devez le désactiver.

La commande infacmd isp RemoveService utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RemoveService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Obligatoire. Nom du service que vous souhaitez supprimer. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.

RemoveServiceLevel

Supprime un niveau de service. Lorsque vous supprimez un niveau de service, le gestionnaire de flux de travail ne met pas à jour les tâches qui l'utilisent. Si aucun niveau de service de flux de travail n'existe dans le domaine, l'équilibrage de charge répartit les tâches avec le niveau de service par défaut.

La commande infacmd isp RemoveServiceLevel utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RemoveServiceLevel :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceLevelName -ln	service_level_name	Obligatoire. Nom du niveau de service que vous souhaitez supprimer.

RemoveUser

Supprime un compte utilisateur du domaine de sécurité natif. Vous ne pouvez pas supprimer de comptes utilisateur dans les domaines de sécurité LDAP.

La commande infacmd isp RemoveUser utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RemoveUser :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_se conds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ExistingUserName -eu	existing_user_name	Obligatoire. Compte utilisateur que vous souhaitez supprimer.

RemoveUserFromGroup

Supprime un utilisateur natif ou LDAP d'un groupe natif dans le domaine.

La commande infacmd isp RemoveUserFromGroup utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RemoveUserFromGroup :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ExistingUserName -eu	existing_user_name	Obligatoire. Nom de l'utilisateur que vous souhaitez supprimer.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur que vous souhaitez supprimer. La valeur par défaut est Natif.
-GroupName -gn	group_name	Obligatoire. Nom du groupe dont vous souhaitez supprimer l'utilisateur.

RemoveUserPermission

Retire une autorisation d'utilisateur sur un objet.

La commande infacmd isp RemoveUserPermission utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et arguments de la commande infacmd isp RemoveUserPermission :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT.
-ExistingUserName -eu	existing_user_name	Obligatoire. Nom de l'utilisateur auquel vous souhaitez attribuer une autorisation sur un objet.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité de l'utilisateur auquel vous souhaitez attribuer une autorisation. La valeur par défaut est Natif.
-ObjectName -on	object_name	Nom de l'objet pour lequel vous souhaitez supprimer l'autorisation d'accès utilisateur.
-ObjectType -ot	object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE	Obligatoire. Type d'objet. Entrez l'une des valeurs suivantes : <ul style="list-style-type: none"> - Service - Licence - Nœud - Grille - Dossier - OSProfile

RemoveUserPrivilege

Supprime un privilège d'un utilisateur du domaine ou d'un utilisateur d'un service d'application dans le domaine.

La commande infacmd isp RemoveUserPrivilege utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RemoveUserPrivilege :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
ExistingUserName -eu	existing_user_name	Obligatoire. Compte utilisateur dont vous supprimez le privilège. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur dont vous supprimez le privilège. La valeur par défaut est Natif.

Option	Argument	Description
-ServiceName -sn	service_name	Obligatoire. Nom de service du domaine ou de l'application dont vous souhaitez afficher les privilèges.
-PrivilegePath -pp	path_of_privilege	<p>Obligatoire. Nom complet du privilège que vous souhaitez attribuer au groupe. Un nom complet inclut le nom du groupe de privilèges et le nom du privilège. folder/create constitue par exemple un nom complet de privilège pour le service de référentiel. Si le nom du privilège comprend des espaces, placez le chemin entre guillemets comme suit :</p> <p>"Runtime Objects/Monitor/Execute/Manage Execution"</p> <p>Si le nom du privilège inclut le caractère spécial « / », faites-le précéder du caractère d'échappement « \ », comme suit :</p> <p>"Model/View Model/Export\ /Import Models"</p>

RenameConnection

Renomme une connexion. Lorsque vous renommez une connexion, les outils Developer et Analyst mettent à jour les tâches qui utilisent la connexion.

Remarque: Les applications déployées et les fichiers de paramètres identifient une connexion par son nom et non par son ID. Par conséquent, lorsque vous renommez une connexion, vous devez redéployer toutes les applications qui utilisent cette connexion. Vous devez également mettre à jour tous les fichiers de paramètres qui utilisent le paramètre de connexion.

La commande infacmd isp RenameConnection utilise la syntaxe suivante :

```

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

```

Le tableau suivant décrit les options et arguments d'infacmd isp RenameConnection :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConnectionName -cn	connection_name	Obligatoire. Nom de connexion existant.
-NewConnectionName -ncn	new_connection_name	Obligatoire. Nouveau nom de connexion. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Le nom ne peut pas dépasser 128 caractères, contenir des espaces, ou contenir les caractères spéciaux suivants : ~ ` ! \$ % ^ & * () - + = { []] \ : ; " ' < , > . ? /

ResetPassword

Réinitialise le mot de passe pour un utilisateur dans le domaine.

La commande infacmd isp ResetPassword utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp ResetPassword :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-ResetUserName -ru	reset_user_name	Obligatoire. Nom de l'utilisateur dont vous souhaitez réinitialiser le mot de passe.
-ResetUserPassword -rp	reset_user_password	<p>Obligatoire. Nouveau mot de passe de l'utilisateur. Vous pouvez définir un mot de passe avec l'option -rp ou la variable d'environnement INFA_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -rp est prioritaire.</p> <p>Pour un compte utilisateur natif, si vous activez la complexité du mot de passe, utilisez les directives suivantes lorsque vous créez ou modifiez un mot de passe :</p> <ul style="list-style-type: none"> - Le mot de passe doit contenir au moins huit caractères. - Il doit être composé d'un caractère alphabétique, d'un caractère numérique et d'un caractère non alphanumérique, tels que : <pre>! \ " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { } ~</pre> <p>Lorsque vous utilisez des caractères spéciaux dans un mot de passe, il arrive que l'interpréteur de commandes les lise différemment. Par exemple, \$ est interprété comme une variable. Dans ce cas, utilisez un caractère d'échappement pour échapper le caractère spécial.</p>

RunCPUProfile

Calcule le profil du processeur pour un nœud.

Remarque: L'exécution de cette commande prend environ 5 minutes et utilise 100 % d'un processeur sur la machine.

La commande infacmd isp RunCPUProfile utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp RunCPUProfile :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NodeName -nn	node_name	Obligatoire. Nom du nœud pour lequel vous souhaitez calculer le profil du processeur.

SetConnectionPermissions

Assigne des autorisations sur une connexion à un utilisateur ou un groupe après avoir supprimé les précédentes.

La commande infacmd isp SetConnectionPermissions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp SetConnectionPermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.</p>
-RecipientUserName -run	recipient_user_name	Obligatoire si vous ne spécifiez pas le nom du groupe destinataire. Nom de l'utilisateur auquel vous souhaitez attribuer des autorisations pour la connexion
-RecipientGroupName -rgn	recipient_group_name	Obligatoire si vous ne spécifiez pas le nom d'utilisateur du destinataire. Nom du groupe dont les autorisations de la connexion doivent être attribuées.
-RecipientSecurityDomain -rsd	recipient_security_domain_name	Obligatoire si le destinataire appartient à un domaine de sécurité LDAP. Nom du domaine de sécurité auquel appartient le destinataire. La valeur par défaut est Natif.
-ConnectionName -cn	connection_name_security_domain	Requis. Nom de la connexion.
-Permission -p	autorisation	<p>Requis. Type d'autorisation à attribuer. Entrez une ou plusieurs des valeurs suivantes, séparées par des espaces :</p> <ul style="list-style-type: none"> - READ - WRITE. Lecture et écriture. - EXECUTE - GRANT. Lecture et accord. - ALL. Lecture, Écriture, Exécution, Accorder

SetRepositoryLDAPConfiguration

Met à jour les options de configuration du serveur LDAP pour un référentiel PowerCenter.

Après avoir installé Informatica, il se peut que vous deviez mettre à jour les informations de connexion entre le référentiel et le service de répertoire externe LDAP.

Utilisez `infacmd isp ListRepositoryLDAPConfiguration` pour afficher les valeurs actuelles pour les options de configuration du serveur LDAP.

La commande `infacmd isp SetRepositoryLDAPConfiguration` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp SetRepositoryLDAPConfiguration :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Option	Argument	Description
-LDAPAddress -la	ldap_server_address	Obligatoire. Nom d'hôte et numéro de port de la machine qui héberge le service d'annuaire LDAP. Généralement, le numéro de port du serveur LDAP est le 389.
-SearchBase -sb	recherche de base	Obligatoire. Nom unique (NU) de l'entrée qui sert de point de départ pour rechercher des noms d'utilisateur dans l'arborescence de l'annuaire LDAP. Le chemin d'accès mentionné dans le nom unique d'un objet permet à LDAP de localiser cet objet dans l'annuaire. Par exemple, dans Microsoft Active Directory, le nom unique d'un objet utilisateur peut être <code>cn=UserName,ou=OrganizationalUnit,dc=DomainName</code> , où la série des noms uniques relatifs indiqués par <code>dc=DomainName</code> identifie le domaine DNS de l'objet.
-SearchScope -ss	champ de recherche	Obligatoire. Portée de la recherche utilisateur. Choisissez l'une des options suivantes : <ul style="list-style-type: none"> - Base. Effectue la recherche dans l'entrée identifiée par la base de recherche. - Un niveau. Effectue la recherche dans toutes les entrées situées un niveau en dessous de l'entrée de base de recherche, sans toutefois inclure cette entrée. - Sous-arborescence. Effectue la recherche dans la sous-arborescence complète, à tous les niveaux situés sous l'entrée de base de recherche.
-LDAPPrincipal -lp	ldap_principal	Obligatoire. Nom unique (NU) de l'utilisateur principal. Le nom d'utilisateur est souvent composé d'un nom commun (CN), d'une organisation (O) et d'un pays (C). Le nom d'utilisateur principal est un utilisateur administratif qui a accès à l'annuaire. Il ne s'agit pas du nom à authentifier. Spécifiez un utilisateur autorisé à lire les entrées des autres utilisateurs dans le serveur LDAP. Omettez cette option pour vous connecter comme utilisateur anonyme. Pour plus d'informations, consultez la documentation du serveur LDAP.
-LDAPCredential -lc	ldap_credential	Obligatoire. Mot de passe de l'utilisateur principal. Vous pouvez définir un mot de passe avec l'option -lc ou la variable d'environnement INFA_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -lc est prioritaire. Omettez cette option pour vous connecter comme utilisateur anonyme.
-LoginAttribute -lt	login_attribute	Obligatoire. Attribut d'annuaire qui contient des noms de connexion.
-LoginFilter -lf	login_filter	Obligatoire. Chaîne de requête LDAP qui permet de filtrer les résultats pour la recherche utilisateur. Le filtre peut spécifier les types d'attribut, les valeurs d'assertion et les critères correspondants. Par exemple, <code>(objectclass=*)</code> recherche tous les objets. <code>(&(objectClass=user)!(cn=susan))</code> lance une recherche dans tous les objets utilisateur sauf « susan ». Pour plus d'informations sur les filtres de recherche, consultez la documentation du serveur LDAP.

Option	Argument	Description
-UseSSL -us	use_ssl	N'utilisez pas cette option. Informatica ne prend pas en charge les serveurs LDAP qui utilisent SSL pour les versions 8.1.1.
-CertificateDatabase -cd	certificate_database_for_ssl	N'utilisez pas cette option. Informatica ne prend pas en charge les serveurs LDAP qui utilisent SSL pour les versions 8.1.1.

ShowLicense

Affiche les détails de la licence. Les détails de la licence affichés correspondent à un résultat cumulatif de toutes les clés de licences appliquées. Le gestionnaire de service met à jour les détails de la licence existants lorsque vous ajoutez une clé incrémentielle à cette licence.

Pour exécuter la commande infacmd isp ShowLicense, vous devez avoir l'autorisation sur la licence.

La commande infacmd isp ShowLicense utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp ShowLicense :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-LicenseName -ln	license_name	Obligatoire. Nom de la licence.

ShutdownNode

Ferme un nœud. Après avoir fermé un nœud, vous pouvez le redémarrer en lançant le service Informatica sur la machine. Vous ne pouvez pas redémarrer de nœud à l'aide de la commande infacmd.

La commande infacmd isp ShutdownNode utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp ShutdownNode :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NodeName -nn	node_name	Obligatoire. Nom du nœud que vous souhaitez arrêter.

SwitchToGatewayNode

Convertit un nœud de travail existant en nœud de passerelle. Le nœud de travail doit avoir le rôle de service activé.

La syntaxe de la commande infacmd isp SwitchToGatewayNode est la suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp SwitchToGatewayNode :

Option	Description
-DomainName -dn	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	Obligatoire si les informations de connectivité de passerelle du fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NodeName -nn	Requis. Nom du nœud que vous souhaitez transformer en nœud de passerelle.
-EnableSaml -saml	Facultatif. Active ou désactive l'authentification SAML dans le domaine Informatica. Définissez cette valeur sur True pour activer l'authentification SAML dans le domaine Informatica. La valeur par défaut est False.

Option	Description
-SamlTrustStoreDir -std	Facultatif. Répertoire contenant le fichier truststore personnalisé requis pour utiliser l'authentification SAML sur le nœud de passerelle. Spécifiez le répertoire uniquement, pas le chemin d'accès complet au fichier. La valeur par défaut du fichier truststore d'Informatica est utilisée si aucun fichier truststore n'est spécifié.
-SamlTrustStorePassword -stp	Obligatoire si vous utilisez un fichier truststore personnalisé pour l'authentification SAML. Mot de passe pour le fichier truststore personnalisé.
-SamlKeyStoreDir -skd	Facultatif. Répertoire contenant le fichier keystore personnalisé requis pour utiliser l'authentification SAML sur le nœud de passerelle. Spécifiez le répertoire uniquement, pas le chemin d'accès complet au fichier.
-SamlKeyStorePassword -skp	Obligatoire si vous utilisez un fichier keystore personnalisé pour l'authentification SAML. Mot de passe du keystore SAML. *
-AdminconsolePort -ap	Port d'accès à Informatica Administrator.
-AdminconsoleShutdownPort -asp	Numéro de port qui contrôle l'arrêt d'Informatica Administrator.
-LogServiceDirectory -ld	Requis. Chemin du répertoire partagé utilisé par le gestionnaire de journaux pour stocker des fichiers d'événements de journal. Vérifiez que la valeur -ld ne correspond pas à la valeur -sld spécifiée ni ne la contient.
-DatabaseTruststorePassword -dbtp	Facultatif. Mot de passe du fichier truststore de la base de données sécurisée. Obligatoire si vous configurez une base de données du référentiel de domaine sécurisé pour le domaine.
-DatabaseTruststoreLocation -dbtl	Chemin et nom du fichier truststore de la base de données sécurisée. Obligatoire si vous configurez une base de données du référentiel de domaine sécurisé pour le domaine.
Remarque : si vous exécutez actuellement des scripts qui utilisent cette commande pour activer un keystore personnalisé pour l'authentification SAML, vous devez les mettre à jour afin d'y inclure cette option.	

SwitchToWorkerNode

Convertit un nœud de passerelle en un nœud de travail. La commande échoue si le nœud à passer est le seul nœud de passerelle du domaine.

Si le nœud fait office de nœud principal de passerelle, vous devez l'arrêter pour pouvoir le convertir en nœud de travail. Arrêtez le nœud et attendez que la passerelle principale bascule sur un autre nœud. Vous pouvez ensuite redémarrer le nœud et exécuter la commande `infacmd isp SwitchToWorkerNode`.

La commande `infacmd isp SwitchToWorkerNode` utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et arguments d'infacmd isp SwitchToWorkerNode :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NodeName -nn	node_name	Obligatoire. Nom du nœud que vous souhaitez transformer en nœud de travail.

SyncSecurityDomains

Synchronise les utilisateurs et les groupes dans un domaine de sécurité avec ceux présents dans le service de répertoire LDAP.

La commande infacmd isp SyncSecurityDomains utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments de la commande `infacmd isp SyncSecurityDomain` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-SynchronizingNamespace -sn	namespace_to_sync	Nom du domaine de sécurité que vous souhaitez synchroniser avec le service d'annuaire LDAP.
-WaitCompletion -wc	True False	Facultatif. Indique si infacmd attend que la commande soit terminée avant de signaler la réussite ou l'échec de la synchronisation. Si la valeur est True, signale si la commande ne parvient pas à démarrer. Si la commande démarre correctement, indique si la synchronisation réussit ou échoue. Si la valeur est False, indique si la commande démarre correctement ou ne démarre pas, sans attendre que la synchronisation soit terminée. La valeur par défaut est False.

UnassignDefaultOSProfile

Supprime le profil de système d'exploitation par défaut qui est attribué à un utilisateur ou à un groupe.

La syntaxe de la commande infacmd isp UnassignDefaultOSProfile est la suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd isp UnassignDefaultOSProfile` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine.
-RecipientName -nm	nom_destinataire	Requis. Nom d'utilisateur ou nom de groupe auquel attribuer le profil de système d'exploitation par défaut.
-RecipientSecurityDomain -ns	domaine_sécurité_destinataire	Requis si vous utilisez une authentification LDAP et que vous attribuez des autorisations d'utilisateur. Nom du domaine de sécurité auquel appartient l'utilisateur.
-RecipientType -ty	type_destinataire	Requis. Indiquez si le profil de système d'exploitation doit être attribué à un utilisateur ou à un groupe. Entrez l'une des valeurs suivantes : - UserIdentity - GroupIdentity

UnassignISMMSERVICE

Dissocie un service d'intégration PowerCenter d'un service Metadata Manager. Si vous supprimez un service d'intégration PowerCenter, vous devez associer un autre service d'intégration PowerCenter avant de charger des ressources.

La commande `infacmd isp UnassignISMMSERVICE` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments de la commande `infacmd isp UnassignISMMService` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Obligatoire. Nom du service Metadata Manager pour lequel vous souhaitez annuler l'attribution du service d'intégration.
-IntegrationService -is	integration_service_name	Obligatoire. Nom du service d'intégration pour lequel vous souhaitez annuler l'association au service de gestionnaire de métadonnées.

UnassignLicense

Supprime une licence d'un service d'application. Le service doit être arrêté. Après avoir supprimé la licence du service, vous devez assigner une licence valide pour réactiver ce dernier.

La commande UnassignLicense utilise la syntaxe suivante :

```
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 ...
```

Le tableau suivant décrit les options et arguments d'*infacmd isp UnassignLicense* :

Option	Arguments	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <i>infacmd</i> tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, <i>infacmd</i> utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-LicenseName -ln	license_name	Obligatoire. Nom de la licence dont vous souhaitez annuler l'attribution.
-ServiceNames -sn	service_name1 service_name2 ...	Obligatoire. Noms des services pour lesquels vous souhaitez supprimer la licence. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.

UnassignRoleFromGroup

Supprime un rôle d'un groupe pour un domaine ou un service d'application.

La commande infacmd isp UnassignRoleFromGroup utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp UnassignRoleFromGroup :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-GroupName -gn	group_name	Obligatoire. Nom du groupe dont vous souhaitez supprimer un rôle. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-GroupSecurityDomain -gsf	group_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient le groupe dont vous supprimez le rôle. La valeur par défaut est Natif.
-RoleName -rn	role_name	Obligatoire. Nom du rôle que vous souhaitez supprimer du groupe.
-ServiceName -sn	service_name	Obligatoire. Nom du domaine ou du service d'application dont vous souhaitez supprimer le rôle. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.

UnassignRoleFromUser

Supprime un rôle d'un utilisateur pour un domaine ou un service d'application.

La commande infacmd isp UnassignRoleFromUser utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et arguments d'infacmd isp UnassignRoleFromUser :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ExistingUserName -eu	existing_user_Name	Obligatoire. Compte utilisateur dont vous supprimez le rôle. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur dont vous supprimez le rôle. La valeur par défaut est Natif.
-RoleName -rn	role_name	Obligatoire. Nom du rôle que vous souhaitez supprimer de l'utilisateur.
-ServiceName -sn	service_name	Obligatoire. Nom du domaine ou du service d'application dont vous souhaitez supprimer le rôle. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.

UnassignRSWSHubService

Disassocie un référentiel PowerCenter d'un Hub de services Web dans le domaine.

La commande infacmd isp UnassignRSWSHubService utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp UnassignRSWSHubService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Obligatoire. Nom du hub de services Web dont vous souhaitez dissocier un référentiel.
-NodeName -nn	node_name	Obligatoire. Nom du nœud sur lequel s'exécute le processus du hub de services Web. Si l'environnement Informatica est configuré pour une haute disponibilité, cette option spécifie le nom du nœud principal.
-RepositoryService -rs	repository_service_name	Obligatoire. Nom du service de référentiel dont dépend le hub de services Web. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.

UnassociateDomainNode

Dissociez un nœud de domaine de son adresse. Le nom de nœud reste une partie du domaine, mais il ne dispose d'aucune adresse physique.

Par exemple, dans un domaine, « Node1 » est associé à la machine « MyHost:9090 ». Lorsque vous exécutez cette commande, la connexion entre le nom « Node1 » et l'adresse de l'hôte « MyHost:9090 » est supprimée. Vous pouvez ensuite associer « Node1 » à un nouvel hôte. Vous devez exécuter les commandes infasetup DefineGatewayNode ou DefineWorkerNode sur le nouvel hôte pour définir « Node1 » sur cette machine.

La commande `infacmd isp UnassociateDomainNode` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'`infacmd isp UnassociateDomainNode` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NodeName -nn	node_name	Obligatoire. Nom du nœud que vous souhaitez dissocier du domaine.

UpdateConnection

Met à jour une connexion. Pour répertorier des options de connexion, exécutez infacmd isp ListConnectionOptions.

La commande infacmd isp UpdateConnection utilise la syntaxe suivante :

```
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)
```

Le tableau suivant décrit les options et arguments d'infacmd isp UpdateConnection :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ConnectionName -cn	connection_name_security_domain	Obligatoire. Nom de la connexion à mettre à jour.
ConnectionUserName -cun	connection_user_name	Obligatoire. Nom d'utilisateur de la base de données.

Option	Argument	Description
-ConnectionPassword -cpd	connection_passw ord	<p>Obligatoire. Mot de passe pour le nom d'utilisateur de la base de données.</p> <p>Si vous effectuez la mise à jour d'une connexion ADABAS, DB2I, DB2Z, IMS, SEQ ou VSAM, vous pouvez entrer une phrase secrète PowerExchange valide au lieu d'un mot de passe. Les phrases secrètes permettant d'accéder aux bases de données et aux ensembles de données sur z/OS peuvent comporter de 9 à 128 caractères. Les phrases secrètes permettant d'accéder à DB2 for i5/OS peuvent comporter jusqu'à 31 caractères. Les phrases secrètes peuvent contenir les caractères suivants :</p> <ul style="list-style-type: none"> - Lettres majuscules et minuscules - chiffres de 0 à 9 - Espaces - les caractères spéciaux suivants : ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Remarque: le premier caractère est une apostrophe.</p> <p>Les phrases secrètes ne peuvent pas inclure de guillemets simples ('), de guillemets doubles (") ou de symboles de devise.</p> <p>Si une phrase secrète contient des espaces, vous devez la placer entre guillemets doubles ("), par exemple, "Ceci est un exemple de phrase secrète". Si une phrase secrète contient des caractères spéciaux, vous devez l'encadrer par trois guillemets doubles ("""), par exemple, """"Cette phrase secrète contient des caractères spéciaux ! % & * ."""". Si une phrase secrète contient uniquement des caractères alphanumériques sans espaces, vous pouvez l'entrer sans délimiteurs.</p> <p>Remarque: Sur z/OS, une phrase secrète RACF valide peut comporter jusqu'à 100 caractères. PowerExchange tronque les phrases secrètes de plus de 100 caractères lors de leur transmission à RACF pour validation.</p> <p>Pour utiliser des phrases secrètes, vérifiez que l'écouteur PowerExchange est exécuté avec un paramètre de sécurité SECURITY=(1,N) ou supérieur dans le membre DBMOVER. Pour plus d'informations, voir la section du <i>Manuel de référence PowerExchange</i> relative à l'instruction SECURITY.</p> <p>Pour utiliser des phrases secrètes pour les connexions IMS, vérifiez que les conditions supplémentaires suivantes sont respectées :</p> <ul style="list-style-type: none"> - Vous devez configurer l'accès ODBA à IMS comme décrit dans le <i>Guide de l'utilisateur du navigateur PowerExchange</i>. - Vous devez utiliser des cartes de données IMS qui spécifient IMS ODBA comme méthode d'accès. N'utilisez pas de cartes de données qui

Option	Argument	Description
		<p>spécifient la méthode d'accès DL/1 BATCH, car celle-ci nécessite l'utilisation de tâches netport, qui ne prennent pas en charge les phrases secrètes.</p> <ul style="list-style-type: none"> - La base de données IMS doit être en ligne dans la région de contrôle IMS pour que vous puissiez utiliser ODBA pour accéder à IMS.
- Options -o	options	Entrez les paires nom-valeur séparées par des espaces. Pour afficher les options valides, exécutez infacmd isp ListConnectionOptions.

updateCustomLDAPType

Met à jour un type LDAP personnalisé qui définit un service d'annuaire LDAP à partir duquel vous pouvez importer des utilisateurs dans un domaine de sécurité LDAP.

La commande infacmd isp updateCustomLDAPType utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments d'infacmd isp updateCustomLDAPType :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-CustomLDAPTypeName -lt	custom_LDAP_type_name	Obligatoire. Nom du type LDAP personnalisé à mettre à jour.
-DisplayName -dpn	display_name	Facultatif. Nom du type LDAP personnalisé affiché dans l'outil Administrator tool.
-Uid	uid	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient l'identificateur unique (UID) que le gestionnaire de service utilise pour identifier les utilisateurs.
-GroupMembershipAttr -gm	group_membership_attr	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient les informations d'appartenance au groupe d'un utilisateur.
-GroupDescriptionAttr -gd	group_description_attr	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient un texte descriptif sur les groupes dans le service d'annuaire.
-UserSurnameAttr -usn	user_surname_attr	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient le nom d'un utilisateur.
-UserGivenNameAttr -ugn	user_given_name_attr	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient le prénom d'un utilisateur.
-GroupMembershipAttr -gm	LDAP_Group_Membership_Attribute	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient les noms des groupes dans le service d'annuaire.
--UserEmailAttr -ue	user_email_attr	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient l'adresse e-mail d'un utilisateur.
-UserEnableAttr -uen	user_enable_attr	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient
-UserTelephoneAttr -utn	user_telephone_attr	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient le numéro de téléphone d'un utilisateur.
-UserDescriptionAttr -ud	user_description_attr	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient la description d'un utilisateur.

Option	Argument	Description
-CN	cn	Facultatif. Nom de l'attribut dans le service d'annuaire LDAP qui contient l'attribut qui comprend le nom complet ou le nom commun d'un utilisateur.
- FetchRangedAttr -fr	fetch_ranged_attr	Facultatif. Définissez cette option sur True pour récupérer toutes les valeurs contenues dans les attributs à valeurs multiples. Utilisez cette option uniquement avec Microsoft Active Directory.

UpdateDomainOptions

Met à jour les propriétés de domaine. Les propriétés de domaine incluent le délai de résilience, la limite des délais de résilience, le nombre maximal de tentatives de redémarrage, la période de redémarrage, le mode TLS et le mode de répartition.

La commande infacmd isp UpdateDomainOptions utilise la syntaxe suivante :

```
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 ...
```

Le tableau suivant décrit les options et arguments de la commande infacmd isp UpdateDomainOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-DomainOptions -do	option_name=value	Requis. Propriétés de domaine que vous souhaitez mettre à jour. Vous pouvez mettre à jour les propriétés suivantes : <ul style="list-style-type: none"> - LicenseUsageDetailMinDays. Nombre de jours minimum pendant lesquels le gestionnaire de journaux conserve les événements du journal pour utilisation de la licence. - LicenseUsageSummaryMinDays. Nombre de jours minimum pendant lesquels le gestionnaire de journaux conserve les enregistrements de la base de données pour utilisation de la licence. - ResilTimeout. Temps en secondes pendant lequel les services tentent de se connecter en tant que clients à d'autres services. - RestartsMaxAttempts. Nombre de tentatives de redémarrage d'un processus de service d'application par le domaine, sur une période spécifique. - RestartsWithinSeconds. Temps maximal en secondes pendant lequel le domaine tente de redémarrer un processus de service d'application suite à un échec. - ServiceResilTimeout. Durée maximale pendant laquelle le service conserve les ressources pour s'adapter aux délais de résilience. - TaskDispatchMode. Mode de répartition de l'équilibrage de charge pour les tâches : RoundRobin, MetricBased ou Adaptive. Redémarrez le service d'intégration pour appliquer les changements. - TLSMode. Configure la communication sécurisée entre les services à l'intérieur du domaine. Pour appliquer les changements, redémarrez le domaine. Les valeurs valides sont True ou False.

UpdateFolder

Met à jour la description du dossier.

La commande infacmd isp UpdateFolder utilise la syntaxe suivante :

```
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

Le tableau suivant décrit les options et arguments de la commande infacmd isp UpdateFolder :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-FolderPath -fp	full_folder_path	Requis. Chemin d'accès complet, sans le nom de domaine, du dossier que vous souhaitez mettre à jour. Doit être au format suivant : <i>/parent_folder/child_folder</i>
-FolderDescription -fd	description_of_folder	Requis. Description du dossier. Si la description du dossier contient des espaces ou d'autres caractères non alphanumériques, placez-la entre guillemets.

UpdateGatewayInfo

Met à jour les informations de connectivité du nœud de passerelle dans le fichier domains.infa.

Exécutez la commande `infacmd isp UpdateGatewayInfo` pour créer un fichier `domains.infa` ou mettre à jour un fichier `domains.infa` existant. Le fichier `domains.infa` contient les informations de connectivité pour un nœud de passerelle dans un domaine avec la configuration TLS et Kerberos du domaine. Les informations de connectivité comprennent le nom de domaine, le nom d'hôte de domaine et le port HTTP de l'hôte de domaine.

Il se peut que vous deviez générer un fichier `domains.infa` pour exécuter des commandes `infacmd` oie sur une machine cliente. Pour générer le fichier `domains.infa`, exécutez la commande `infacmd isp UpdateGatewayInfo`. La commande `updateGatewayInfo` génère un fichier `domains.infa` dans le répertoire `DeveloperClient`. Définissez le nom d'hôte et le port de la passerelle de domaine lorsque vous exécutez la commande.

La commande `infacmd isp UpdateGatewayInfo` utilise la syntaxe suivante :

```
UpdateGatewayInfo
<-DomainName|-dn> domain_name
<-GatewayAddress|-dg> domain_gateway_host:port
[<-Force|-f>]
```


Le tableau suivant décrit les options et arguments de la commande `infacmd isp UpdateGatewayInfo` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-GatewayAddress -dg	domain_gateway_host:port t	Requis. Nom de machine et numéro de port de l'hôte de passerelle. Entrez l'adresse de la passerelle au format suivant : domain_gateway_host:port
-Force -f	-	Facultatif. Met à jour ou crée le fichier domains.infa, même en cas d'échec de la connexion au domaine. L'option -Force définit les options TLS et Kerberos sur False dans le fichier domains.infa en cas d'échec de la connexion au domaine. Si vous ne spécifiez pas l'option -Force, la commande ne met pas à jour le fichier domains.infa en cas d'échec de la connexion au domaine.

UpdateGrid

Met à jour la liste des nœuds assignés à une grille.

La commande `infacmd isp UpdateGrid` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande `infacmd isp UpdateGrid` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, <code>infacmd</code> utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-GridName -gn	grid_name	Requis. Nom de la grille.

Option	Argument	Description
-NodeList -nl	node1 node2 ...	Requis. Noms des nœuds à attribuer à la grille. Cette liste de nœuds remplace ou met à jour la liste de nœuds précédemment attribuée à la grille en fonction de la définition de l'option -ul. Si l'option -ul est spécifiée, elle met à jour la liste de nœuds précédemment attribuée à la grille. Si l'option -ul n'est pas spécifiée, elle remplace la liste de nœuds précédemment attribuée à la grille.
-UpdateNodeList -ul	True False	Facultatif. Remplace la liste de nœuds actuels par les valeurs de l'option -nl au lieu de remplacer la liste de nœuds précédemment attribuée à la grille. Si cette option est définie sur True, la commande infacmd remplace la liste de nœuds par celle spécifiée à l'aide de l'option -nl ainsi que les nœuds précédemment attribués à la grille. Si elle est définie sur False, la commande infacmd remplace la liste de nœuds par la liste de nœuds spécifiée à l'aide de l'option -nl. La valeur par défaut est False.

UpdateIntegrationService

Met à jour les propriétés de configuration pour le service PowerCenter Integration Service.

La commande infacmd isp UpdateIntegrationService utilise la syntaxe suivante :

```
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 ...]
```

Remarque: Pour infacmd isp UpdateIntegrationService, vous ne devez pas utiliser les options -ru, -rp et -rsdn dans l'authentification Kerberos. Si vous utilisez ces options en mode Kerberos, la commande échoue.

Le tableau suivant décrit les options et arguments de la commande `infacmd isp UpdateIntegrationService` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir une connexion au domaine. Si vous omettez cette option, <code>infacmd</code> utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.

Option	Argument	Description
-NodeName -nn	node_name	Facultatif. Nom du nœud sur lequel s'exécute le processus de service d'intégration. Si l'environnement PowerCenter est configuré pour une haute disponibilité, il s'agit du nom du nœud principal. N'entrez aucune valeur pour cette option si vous spécifiez le nom de la grille.
-GridName -gn	grid_name	Facultatif. Nom de la grille sur laquelle s'exécute le processus de service d'intégration. N'entrez aucune valeur pour cette option si vous spécifiez le nom du nœud.
-BackupNodes -bn	node1 node2 ...	Facultatif. Nœuds sur lesquels le processus de service peut s'exécuter lorsque le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.
-RepositoryService -rs	repository_service_name	Facultatif. Nom du service de référentiel dont dépend le service d'intégration. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-RepositoryUser -ru	user	Obligatoire pour l'authentification native ou LDAP. Nom d'utilisateur utilisé pour la connexion au référentiel. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-RepositoryPassword -rp	mot de passe	Obligatoire pour l'authentification native ou LDAP. Mot de passe de l'utilisateur. Vous pouvez définir un mot de passe avec l'option -rp ou la variable d'environnement INFA_REPOSITORY_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -rp est prioritaire.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Obligatoire pour l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel appartient l'utilisateur du référentiel PowerCenter. Le nom du domaine de sécurité est sensible à la casse. Si vous ne spécifiez pas cette option, la commande définit le domaine de sécurité de l'utilisateur du référentiel sur natif.
-ServiceOptions -so	option_name=value	Facultatif. Propriétés des services qui définissent la manière dont le service d'intégration PowerCenter est exécuté.

updateLDAPConnectivity

Met à jour la configuration LDAP spécifiée.

La commande infacmd isp updateLDAPConnectivity utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et les arguments d'infacmd isp updateLDAPConnectivity :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-LDAPAddress -la	ldap_server_address	Obligatoire. Nom d'hôte et numéro de port de la machine qui héberge le service d'annuaire LDAP. Généralement, le numéro de port du serveur LDAP est le 389. Si le serveur LDAP utilise SSL, le numéro de port du serveur LDAP est le 636.
-LDAPPrincipal -lp	ldap_principal	Facultatif. Nom unique (NU) de l'utilisateur principal. Omettez cette option pour vous connecter comme utilisateur anonyme. Pour plus d'informations, consultez la documentation du service d'annuaire LDAP.
-LDAPCredential -lc	ldap_credential	Facultatif. Mot de passe de l'utilisateur principal. Vous pouvez définir un mot de passe avec l'option -lc ou la variable d'environnement INFA_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -lc est prioritaire. Omettez cette option pour vous connecter comme utilisateur anonyme.
-UseSSL -us	use_ssl	Facultatif. Si vous incluez l'option, le service d'annuaire LDAP utilise le protocole Secure Sockets Layer (SSL).

Option	Argument	Description
-TrustLDAPCertificate -tc	trust_ldap_certificate	Facultatif. Si vous incluez l'option, PowerCenter se connecte au serveur LDAP sans vérifier le certificat SSL. Si vous n'incluez pas l'option, PowerCenter vérifie que le certificat SSL est signé par une autorité de certification avant de se connecter au serveur LDAP.
-LDAPType -lt	ldap_types=value	Obligatoire. Type de service d'annuaire LDAP. Les services d'annuaire incluent : <ul style="list-style-type: none"> - MicrosoftActiveDirectory - Microsoft Azure Active Directory - SunJavaSystemDirectory - NovellE-Directory - IBMTivoliDirectory - OpenLDAP - Oracle Directory Server (ODSEE) - Oracle Unified Directory Si vous utilisez un service d'annuaire LDAP personnalisé, spécifiez le nom du service.
-MaxSecurityDomainSize -ms	Max_Security_Domain_size	Facultatif. Nombre maximal de comptes utilisateur à importer dans un domaine de sécurité. La valeur par défaut est 1 000.
-GroupMembershipAttr -gm	LDAP_Group_Membership_Attribute	Facultatif. Nom de l'attribut qui contient des informations d'appartenance au groupe pour un utilisateur.
-LDAPNotCaseSensitive -lnc	LDAP_Not_Case_Sensitive	Facultatif. Indique que les noms d'utilisateur provenant du service d'annuaire LDAP ne sont pas sensibles à la casse. La valeur par défaut est False.
-LDAPHostConfigurationName -lcn	LDAP_host_configuration_name	Obligatoire. Nom de la configuration LDAP à mettre à jour.

UpdateLicense

Met à jour les informations de la licence pour le domaine. Exécutez cette commande pour mettre à niveau votre licence à l'aide d'une clé de licence incrémentielle. Utilisez la clé pour ajouter ou supprimer les options sous licence.

Lorsque vous ajoutez une clé incrémentielle à une licence, le gestionnaire de service met à jour la date d'expiration de la licence si la date d'expiration de la clé incrémentielle est postérieure à celle de la clé d'origine.

La commande `infacmd isp UpdateLicense` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments de la commande `infacmd isp UpdateLicense` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-LicenseName -ln	license_name	Obligatoire. Nom de l'objet licence que vous souhaitez mettre à jour.
-LicenseKeyFile -lf	license_key_file	Obligatoire. Nom et chemin du fichier qui contient les clés incrémentielles.

UpdateMMService

Met à jour ou crée les options de service pour un service Metadata Manager. Pour mettre à jour ou créer les options de service, désactivez le service Metadata Manager, mettez à jour les options et réactivez le service.

La commande infacmd isp UpdateMMService utilise la syntaxe suivante :

```
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 ...>
```

Le tableau suivant décrit les options et arguments d'infacmd isp UpdateMMService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Obligatoire. Nom du service de gestionnaire de métadonnées que vous souhaitez mettre à jour.

Option	Argument	Description
-LicenseName -ln	license_name	Obligatoire. Nom de la licence que vous voulez assigner au service de gestionnaire de métadonnées.
-ServiceOptions -so	option_name=value	Facultatif. Propriétés du service qui définissent la manière d'exécuter le service de gestionnaire de métadonnées.

UpdateMonitoringOptions

Met à jour les propriétés générales pour contrôler les actions du domaine.

Lorsque vous spécifiez un service de référentiel modèle avec l'option -ModelRepositoryService, vous devez également entrer des valeurs pour les options -RepositoryUserName et -RepositoryPassword. Vous devez inclure des valeurs pour les trois options ou pour aucune d'elles.

La commande infacmd isp UpdateMonitoringOptions utilise la syntaxe suivante :

```
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)]
```

Le tableau suivant décrit les options et arguments d'infacmd isp UpdateMonitoringOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est la zone de l'utilisateur spécifiée lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel la commande infacmd tente d'établir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire. La valeur par défaut est 180 secondes.
-ModelRepositoryService -rs	model_repository_service	Facultatif. Nom du service de référentiel modèle qui stocke les informations de l'historique.
-RepositoryUserName -rsun	model_repository_user_name	Requis pour l'authentification native ou LDAP. Facultatif si le domaine utilise l'authentification Kerberos. Nom d'utilisateur permettant l'accès au service de référentiel modèle.
-RepositoryPassword -rspd	model_repository_password	Requis pour l'authentification native ou LDAP. Facultatif si le domaine utilise l'authentification Kerberos. Mot de passe d'utilisateur permettant l'accès au service de référentiel modèle.
-RepositorySecurityDomain -rsdn	model_repository_security_domain	Requis pour l'authentification LDAP ou Kerberos. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel appartient l'utilisateur du référentiel PowerCenter. Le domaine de sécurité est sensible à la casse. Si vous ne spécifiez pas cette option, la commande définit le domaine de sécurité de l'utilisateur du référentiel sur Natif.
-AdministratorOptions -ao	option_name=value	Facultatif. Paramètres d'administration générale des enregistrements et des rapports de surveillance. Vous pouvez définir les options suivantes : <ul style="list-style-type: none"> - MaxSortedRecords. Nombre maximal d'enregistrements pouvant être triés. La valeur par défaut est 3 000. - ShowMilliseconds. Inclure les millisecondes dans les champs de date et heure des rapports de surveillance. Vous pouvez définir la valeur sur « True » ou « False ». La valeur par défaut est False.

Option	Argument	Description
-CachingOption -co	option_name=value	Facultatif. Paramètres de mise en cache des statistiques. Vous pouvez définir les options suivantes : <ul style="list-style-type: none"> - DefaultNotificationDelay. Nombre maximal de secondes pendant lesquelles le service d'intégration de données met en mémoire tampon les statistiques avant de les conserver dans le référentiel modèle et de les écrire dans un rapport de surveillance. La valeur par défaut est 10.
-PurgeOptions -po	option_name=value	Facultatif. Paramètres de purge des statistiques. Vous pouvez définir les options suivantes : <ul style="list-style-type: none"> - PurgeScheduleTime. Heure du jour à laquelle le service de référentiel modèle purge les statistiques. La valeur par défaut est 01:00. - PurgeTaskFrequency. Intervalle de temps, en jours, entre lesquels le service de référentiel modèle purge les statistiques plus anciennes que les valeurs configurées pour les options ExpiryTime. La valeur par défaut est 1. - StatisticsExpiryTime. Nombre de jours pendant lesquels le référentiel modèle enregistre des statistiques moyennes. Si la purge est désactivée, le référentiel modèle enregistre les statistiques indéfiniment. La valeur par défaut est 180. La valeur minimale est 0. La valeur maximale est 366. - DetailedStatisticsExpiryTime. Nombre de jours pendant lesquels le référentiel modèle enregistre des statistiques par minute. Si la purge est désactivée, le référentiel modèle enregistre les statistiques indéfiniment. La valeur par défaut est 14. La valeur minimale est 1. La valeur maximale est 14.

UpdateNamespace

Met à jour un domaine de sécurité LDAP avec les filtres fournis pour l'utilisateur et le groupe. Met à jour le domaine de sécurité LDAP si le domaine Informatica utilise l'authentification LDAP ou Kerberos.

La commande infacmd isp UpdateNamespace utilise la syntaxe suivante :

```
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]

```

Le tableau suivant décrit les options et les arguments d'infacmd isp UpdateNamespace :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Vous pouvez spécifier une valeur pour -sdn ou utiliser la valeur par défaut selon le mode d'authentification : <ul style="list-style-type: none"> - Requis si le domaine utilise l'authentification LDAP. La valeur par défaut est Natif. Pour travailler avec l'authentification LDAP, vous devez spécifier la valeur pour -sdn. - Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. La valeur par défaut est natif pour l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd essaye d'établir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous ne spécifiez pas la variable d'environnement, la valeur par défaut utilisée est de 180 secondes.
-NameSpace -ns	namespace	Requis. Nom du domaine de sécurité LDAP ou Kerberos. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Le nom ne peut pas contenir d'espaces ou les caractères spéciaux suivants : , + / < > @ ; \ % ? Le nom ne peut pas dépasser 128 caractères. Le nom peut inclure des espaces ASCII, sauf en première et dernière position. Vous ne pouvez pas utiliser d'autres caractères d'espace.
-UserSearchBase -usb	usersearchbasesu	Le nom unique (DN) de l'entrée sert de point de départ pour rechercher les noms d'utilisateurs dans le service d'annuaire LDAP. Le service d'annuaire LDAP recherche un objet dans le répertoire selon le chemin d'accès dans le nom unique de l'objet. Par exemple, dans Microsoft Active Directory, le nom unique d'un objet utilisateur peut être cn=UserName,ou=OrganizationalUnit,dc=DomainName. La série des noms uniques relatifs indiqués par dc=DomainName identifie le domaine DNS de l'objet.
-UserFilter -uf	userfilter	Chaîne de requête LDAP qui spécifie les critères de recherche pour rechercher des utilisateurs dans le service d'annuaire. Le filtre peut indiquer les types d'attributs, les valeurs d'assertion et les critères de correspondance. Par exemple : le filtre (objectclass=*) recherche tous les objets. Le filtre (&(objectClass=user)(!(cn=susan))) recherche tous les objets utilisateurs sauf « susan ». Pour plus d'informations sur les filtres de recherche, consultez la documentation du service d'annuaire LDAP.
-GroupSearchBase -gsb	groupsearchbase	Le nom unique (DN) de l'entrée sert de point de départ pour rechercher les noms de groupes dans le service d'annuaire LDAP.
-GroupFilter -gf	groupfilter	Chaîne de requête LDAP qui spécifie les critères de recherche pour les groupes dans le service d'annuaire.
-LDAPHostConfigurationName -lcn	ldapName	Facultatif. Nom de la configuration LDAP associée au domaine de sécurité.

UpdateNodeOptions

Met à jour les propriétés générales du nœud telles que le répertoire de sauvegarde, le profil du processeur, le niveau de gravité de l'erreur, les ports du processus de service et le seuil de fourniture de ressources.

La commande infacmd isp UpdateNodeOptions utilise la syntaxe suivante :

```
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 ...]
```

Le tableau suivant décrit les options et arguments de la commande infacmd isp UpdateNodeOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NodeName -nn	node_name	Facultatif. Nom du nœud dont vous souhaitez mettre à jour les seuils de fourniture de ressources.

Option	Argument	Description
-NodeOptions -no	option_name=value	<p>Facultatif. Options du nœud que vous souhaitez mettre à jour. Vous pouvez mettre à jour les options suivantes :</p> <ul style="list-style-type: none"> - BackupDir. Répertoire de stockage des fichiers de sauvegarde du référentiel. - CPUProfile. Classement des performances du processeur du nœud par rapport à un système de base. ErrorSeverityLevel. Niveau de journalisation des erreurs du nœud : error, warning, info, trace, debug. - MaxProcessPort. Numéro de port maximum utilisé par les processus de service sur le nœud. - MinProcessPort. Numéro de port minimum utilisé par les processus de service sur le nœud. <p>L'exemple suivant affecte le port 1515 à MaxProcessPort :</p> <pre>infacmd UpdateNodeOptions ... -no MaxProcessPort=1515</pre>
-ResourceProvision -rp	option_name=value	<p>Facultatif. Seuils de fourniture de ressources que vous souhaitez mettre à jour. Vous pouvez mettre à jour les seuils suivants :</p> <ul style="list-style-type: none"> - MaxCPURunQueueLength. Nombre maximal de threads exécutables en attente de ressources du processeur sur le nœud. - MaxMemoryPercent. Pourcentage maximum de mémoire virtuelle alloué au nœud par rapport à la taille totale de la mémoire physique. - MaxProcesses. Nombre maximal de tâches Session et Command qui peuvent être exécutées sur chaque service d'intégration exécuté sur le nœud. <p>L'exemple suivant affecte la valeur 15 à MaxProcess :</p> <pre>infacmd UpdateNodeOptions ... -rp MaxProcesses=15</pre>

UpdateNodeRole

Met à jour le rôle sur un nœud du domaine. Vous pouvez activer ou désactiver le rôle de service ou le rôle de calcul sur un nœud.

Par défaut, chaque nœud est doté des rôles de service et de calcul. Si un nœud est attribué à une grille du service d'intégration de données, vous pouvez éventuellement mettre son rôle à jour. Activez uniquement le rôle de service pour dédier le nœud à l'exécution du processus de service d'intégration de données. Activez uniquement le rôle de calcul pour dédier le nœud à l'exécution de mappages du service d'intégration de données.

Si vous mettez à jour le rôle sur un nœud attribué à un service d'intégration de données ou à une grille du service d'intégration de données, vous devez redémarrer le service d'intégration de données pour appliquer les modifications.

La commande `infacmd isp UpdateNodeRole` utilise la syntaxe suivante :

```
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]

```

Le tableau suivant décrit les options et les arguments de la commande `infacmd isp UpdateNodeRole` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-NodeName -nn	node_name	Requis. Nom du nœud que vous souhaitez mettre à jour.
-EnableServiceRole -esr	True False	<p>Facultatif. Active le rôle de service sur le nœud. Si la valeur est True, les services d'application peuvent s'exécuter sur le nœud. Si la valeur est False, les services d'application ne peuvent pas s'exécuter sur le nœud. Définissez cette valeur sur False uniquement si le nœud est attribué à une grille du service d'intégration de données si vous souhaitez le dédier à l'exécution de mappages.</p> <p>La valeur par défaut est True.</p>

Option	Argument	Description
-EnableComputeRole -esr	True False	Facultatif. Active le rôle de calcul sur le nœud. Si la valeur est True, le nœud peut effectuer des calculs demandés par des services d'application distants. Si la valeur est False, le nœud ne peut pas effectuer de calculs demandés par des services d'application distants. Un nœud doit être doté du rôle de calcul si le service d'intégration de données y exécute des tâches. Si le service d'intégration de données n'exécute pas de tâches sur le nœud, vous pouvez désactiver le rôle de calcul. Cependant, l'activation et la désactivation du rôle de calcul n'ont aucun impact sur les performances. La valeur par défaut est True.
-disableComputeRoleMode -mo	disable_mode	Facultatif. Définit la manière dont le rôle de calcul est désactivé : <ul style="list-style-type: none"> - Terminer. Permet l'exécution complète des calculs avant la désactivation du rôle de calcul. - Arrêter. Arrête l'exécution des calculs puis désactive le rôle de calcul. - Abandonner. Tente d'arrêter toutes les exécutions de calculs avant de les abandonner et de désactiver le rôle de calcul. La valeur par défaut est Abandonner.

UpdateOSProfile

Met à jour les propriétés d'un profil de système d'exploitation dans le domaine.

Remarque: Pour exécuter des flux de travail utilisant des profils de système d'exploitation, vous devez disposer de l'option Profils des systèmes d'exploitation.

La commande infacmd isp UpdateOSProfile utilise la syntaxe suivante :

```
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 ...]
```

Le tableau suivant décrit les options et arguments d'infacmd isp UpdateOSProfile :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-OSProfileName -on	OSProfile_name	Requis. Nom du profil de système d'exploitation.
-IntegrationServiceProcessOptions -po	option_name=value	Facultatif. Propriétés de service qui définissent le mode d'exécution du service d'intégration PowerCenter.
-EnvironmentVariables -ev	nom=valeur	Facultatif. Nom et valeur des variables d'environnement utilisées par le service d'intégration PowerCenter lors de l'exécution.
-DISProcessVariables -diso	option_name=value	Facultatif. Propriétés du processus de service qui définissent le mode d'exécution du service d'intégration de données.
-DISEnvironmentVariables -dise	nom=valeur	Facultatif. Nom et valeur des variables d'environnement utilisées par le service d'intégration de données lors de l'exécution.
-HadoopImpersonationProperties -hipr	hadoop_impersonation_properties	Facultatif. Indique si le service d'intégration de données utilise l'utilisateur d'emprunt d'identité Hadoop pour exécuter des mappages, des flux de travail et des tâches de profilage dans un environnement Hadoop. Les valeurs valides sont True ou False.
-HadoopImpersonationUser -hu	hadoop_impersonation_user	Facultatif. Entrez le nom d'utilisateur dont le service d'intégration de données emprunte l'identité lorsqu'il exécute des tâches dans un environnement Hadoop.
-UseLoggedInUserAsProxy -ip	use_logged_in_user_as_proxy	Facultatif. Indique si vous souhaitez utiliser l'utilisateur connecté en tant qu'utilisateur d'emprunt d'identité Hadoop. Les valeurs valides sont True ou False.

Option	Argument	Description
-ProductExtensionName -pe	product_extension_name	Facultatif. Réserve pour une utilisation ultérieure.
-ProductOptions -o	optionGroupName.optionName=Value	<p>Obligatoire. Nom et valeur de chaque option définie. Utilisez l'option permettant de créer un répertoire du cache de fichier plat que le profil du système d'exploitation peut utiliser.</p> <p>Par exemple, la commande suivante définit le répertoire du cache sur \$PMRootDir/OSPCache:</p> <pre>infacmd isp createOSProfile ... -o 'runTimeVariables.flatFileCacheDirectory'="\$PMRootDir/OSPCache"</pre>

UpdateRepositoryService

Met à jour ou crée des options de service pour le service de référentiel PowerCenter.

Par exemple, vous pouvez mettre à jour le mode de fonctionnement du service de référentiel PowerCenter et le définir sur Normal ou Exclusif. Le mode Normal permet à plusieurs utilisateurs d'accéder au service de référentiel PowerCenter et de mettre à jour son contenu. Le mode Exclusif autorise un seul utilisateur à accéder au service de référentiel PowerCenter et à mettre à jour son contenu. Paramétrez le mode de fonctionnement sur exclusif lorsque vous effectuez des tâches d'administration qui nécessitent la connexion et la mise à jour de la configuration par un seul utilisateur. Pour mettre à jour le mode de fonctionnement du service de référentiel PowerCenter, désactivez le service, mettez à jour le mode de fonctionnement et réactivez le service.

La commande `infacmd isp UpdateRepositoryService` utilise la syntaxe suivante :

```
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 ...]
```

Le tableau suivant décrit les options et arguments de la commande `infacmd isp UpdateRepositoryService` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, <code>infacmd</code> utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel PowerCenter à mettre à jour. Pour saisir un nom contenant une espace ou tout autre caractère non alphanumérique, placez-le entre guillemets.

Option	Argument	Description
-NodeName -nn	node_name	Facultatif. Nom du nœud sur lequel s'exécute le processus de service du référentiel PowerCenter. Si l'environnement PowerCenter est configuré pour une haute disponibilité, il s'agit du nom du nœud principal.
-BackupNodes -bn	node1 node2 ...	Facultatif. Nœuds sur lesquels le processus de service peut s'exécuter lorsque le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.
-ServiceOptions -so	option_name=value	Requis. Propriétés du service qui définissent le mode d'exécution du service de référentiel PowerCenter.

Options de service de référentiel (-so)

Entrez les options de service de référentiel au format suivant :

```
infacmd CreateRepositoryService ... -so option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options du service de référentiel :

Option	Description
AllowWritesWithRACaching	Facultatif. Utilise les outils clients PowerCenter pour modifier les métadonnées du référentiel lorsque la mise en cache de RepAgent est activée. La valeur par défaut est Oui.
CheckinCommentsRequired	Facultatif. Les utilisateurs doivent ajouter des commentaires lors de l'archivage d'objets du référentiel. La valeur par défaut est Oui. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.
CodePage	Requis. Description de la page de code de la base de données. Pour saisir une description de page de code contenant une espace ou tout autre caractère non alphanumérique, placez son nom entre guillemets.
ConnectionString	Requis. Chaîne de connexion de la base de données spécifiée lors de la configuration du service de référentiel PowerCenter. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.
DBPassword	Requis. Mot de passe de l'utilisateur de la base de données du référentiel. Vous pouvez définir un mot de passe avec l'option -so ou la variable d'environnement INFA_DEFAULT_DATABASE_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -so est prioritaire. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.
DBPoolExpiryThreshold	Facultatif. Nombre minimal de connexions de base de données inactives autorisé par le service de référentiel PowerCenter. Par exemple, si 20 connexions sont inactives et que vous réglez ce seuil sur 5, le service de référentiel PowerCenter ne ferme pas plus de 15 connexions. La valeur minimale est 3. La valeur par défaut est 5.

Option	Description
DBPoolExpiryTimeout	Facultatif. Intervalle, en secondes, pendant lequel le service de référentiel PowerCenter recherche des connexions de base de données inactives. Si une connexion est inactive pour une durée supérieure à cette valeur, le service de référentiel PowerCenter peut fermer la connexion. La valeur minimale est 300. La valeur maximale est 2 592 000 (30 jours). La valeur par défaut est 3 600 (1 heure).
DBUser	Requis. Compte de la base de données contenant le référentiel. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.
DatabaseArrayOperationSize	Facultatif. Nombre de lignes à récupérer à chaque opération sur une base de données de tableau (insertion ou récupération, par exemple). La valeur par défaut est 100. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.
DatabaseConnectionTimeout	Facultatif. Temps en secondes pendant lequel le service de référentiel PowerCenter tente d'établir une connexion au système de gestion de base de données. La valeur par défaut est 180.
DatabasePoolSize	Facultatif. Nombre maximal de connexions à la base de données du référentiel que le service de référentiel PowerCenter est capable d'établir. La valeur minimale est 20. La valeur par défaut est 500.
DatabaseType	Requis. Type de base de données qui contient les métadonnées du référentiel. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.
EnableRepAgentCaching	Facultatif. Active la fonctionnalité de mise en cache de l'agent du référentiel. La valeur par défaut est Oui.
ErrorSeverityLevel	Facultatif. Niveau minimal des messages d'erreur écrits dans le journal du service de référentiel PowerCenter : <ul style="list-style-type: none"> - Irrécupérable - Erreur - Avertissement - Informations - Trace - Déboguer La valeur par défaut est Informations.
HeartBeatInterval	Facultatif. Intervalle pendant lequel le service de référentiel PowerCenter vérifie sa connexion aux clients du service. La valeur par défaut est 60 secondes.
MaxResilienceTimeout	Facultatif. Délai maximal, en secondes, pendant lequel le service conserve les ressources à des fins de résilience. La valeur par défaut est 180.
MaximumConnections	Facultatif. Nombre maximal de connexions que le référentiel accepte des clients du référentiel. La valeur par défaut est 200.
MaximumLocks	Facultatif. Nombre maximal de verrous que le référentiel place sur les objets de métadonnées. La valeur par défaut est 50 000.

Option	Description
OperatingMode	Facultatif. Mode d'exécution du service de référentiel PowerCenter : <ul style="list-style-type: none"> - Normal - Exclusif La valeur par défaut est Normal. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.
OptimizeDatabaseSchema	Facultatif. Permet d'optimiser le schéma de base de données du référentiel lors de la création du contenu du référentiel ou de la sauvegarde et de la restauration d'un référentiel IBM DB2 ou Microsoft SQL Server. Une fois activé, le service de référentiel PowerCenter tente de créer les tables de référentiel qui contiennent des colonnes Varchar avec une précision de 2000 au lieu de colonnes CLOB. Utilisez les colonnes Varchar pour augmenter les performances du référentiel. Lors de l'utilisation des colonnes Varchar, vous devez réduire les entrées et sorties disque et la base de données peut mettre les colonnes en cache. Pour utiliser cette option, vérifiez la taille de page requise pour les bases de données de référentiel suivantes : <ul style="list-style-type: none"> - IBM DB2. La taille de page de la base de données doit être supérieure ou égale à 4 Ko. Au minimum, un espace de table temporaire ayant une taille de page supérieure ou égale à 16 Ko. - Microsoft SQL Server. La taille de page de la base de données doit être supérieure ou égale à 8 Ko. La valeur par défaut est désactivée.
PreserveMXData	Facultatif. Conserve les données MX pour les versions antérieures des mappages. La valeur par défaut est désactivée.
RACacheCapacity	Facultatif. Nombre d'objets que le cache peut contenir lorsque la mise en cache de l'agent du référentiel est activée. La valeur par défaut est 10 000.
SecurityAuditTrail	Facultatif. Permet le suivi des modifications apportées aux utilisateurs, aux groupes, aux privilèges et aux autorisations. La valeur par défaut est Non.
ServiceResilienceTimeout	Facultatif. Période (en secondes) pendant laquelle le service tente d'établir ou de rétablir une connexion à un autre service. La valeur par défaut est 180. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.
TableOwnerName	Facultatif. Nom du propriétaire des tables de référentiel pour un référentiel IBM DB2.
TablespaceName	Facultatif. Nom de l'espace de table pour les référentiels IBM DB2. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.
TrustedConnection	Facultatif. Utilise l'authentification Windows pour accéder à la base de données Microsoft SQL Server. La valeur par défaut est Non. Pour appliquer les modifications, redémarrez le service de référentiel PowerCenter.

UpdateSAPBWService

Met à jour le service et les options de processus de service pour le service SAP BW.

La commande infacmd isp UpdateSAPBWService utilise la syntaxe suivante :

```
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 ...]
```

Le tableau suivant décrit les options et arguments d'infacmd isp UpdateSAPBWService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Obligatoire. Nom du service SAP BW. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-NodeName -nn	node_name	Facultatif. Nom du nœud sur lequel s'exécute le processus du service SAP BW. Si l'environnement PowerCenter est configuré pour une haute disponibilité, il s'agit du nom du nœud principal.
-ServiceOptions -so	option_name=value	Facultatif. Propriétés du service qui définissent le mode d'exécution du service SAP BW.
-ServiceProcessOptions -po	option_name=value	Facultatif. Propriétés du processus de service qui définissent le mode d'exécution du processus de service SAP BW.

UpdateServiceLevel

Met à jour les propriétés du niveau de service. Vous pouvez mettre à jour la priorité de répartition et le temps d'attente de répartition maximal.

La commande infacmd isp UpdateServiceLevel utilise la syntaxe suivante :

```
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 ...
```

Le tableau suivant décrit les options et arguments d'infacmd isp UpdateServiceLevel :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceLevelName -ln	service_level_name	Obligatoire. Nom du niveau de service que vous souhaitez mettre à jour.
-ServiceLevel -sl	option_name=value	Obligatoire. Propriétés du niveau de service que vous souhaitez mettre à jour. Vous pouvez mettre à jour les propriétés suivantes : <ul style="list-style-type: none"> - DispatchPriority. Priorité initiale de répartition. Les numéros les plus petits ont une priorité plus élevée. La priorité 1 est la plus élevée. - MaxDispatchWaitTime. Délai en secondes qui peut s'écouler avant que l'équilibrage de charge ne remonte la priorité de répartition d'une tâche vers la priorité la plus élevée.

UpdateServiceProcess

Met à jour les valeurs des options du processus de service d'intégration PowerCenter.

La commande infacmd isp UpdateServiceProcess utilise la syntaxe suivante :

```
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 ...]
```

Le tableau suivant décrit les options et arguments de la commande `infacmd isp UpdateServiceProcess` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Obligatoire. Nom du service. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-NodeName -nn	node_name	Obligatoire. Nom du nœud sur lequel vous souhaitez mettre à jour les informations de configuration.
-ServiceProcessOptions -po	option_name=value	Nom et nouvelles valeurs des options dont vous souhaitez mettre à jour les valeurs. Vous pouvez spécifier plusieurs paires option_name=value. Vous pouvez utiliser une variable de processus dans la valeur. Par exemple, la commande suivante affecte « \$PMRootDir/NewCache » au répertoire de cache et « \$PMRootDir/NewBadFiles » au répertoire du fichier de rejet : <pre>infacmd UpdateServiceProcess ... -po \$PMCacheDir=\$PMRootDir/NewCache \$PMBadFileDir= \$PMRootDir/NewBadFiles</pre> Obligatoire si vous ne spécifiez pas ProcessEnvironmentVariables.
-ProcessEnvironmentVariables -ev	option_name=value	Variables d'environnement du processus de service. Vous pouvez spécifier plusieurs variables d'environnement. Par exemple, la commande suivante ajoute ou met à jour le répertoire JAVA_HOME sur « \$HOME/java » et le répertoire INFA_HOME sur « \$HOME/Informatique/9.0.1/install » pour le processus de service spécifié : <pre>infacmd ProcessEnvironmentVariables ... -ev JAVA_HOME=\$HOME/java INFA_HOME=\$HOME/ Informatique/9.0.1/install</pre> Obligatoire si vous ne spécifiez pas ServiceProcessOptions.

UpdateSMTPOptions

Met à jour la configuration SMTP du domaine. La configuration SMTP est utilisée pour envoyer des alertes de domaine et des notifications de fiche d'évaluation.

Après avoir configuré les paramètres SMTP, vous devez inscrire l'utilisateur aux alertes en utilisant la commande AddAlertUser.

La syntaxe de la commande infacmd isp UpdateSMTPOptions est la suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd isp UpdateSMTPOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Password -pd	password	Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Native.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-SMTPAddress -sa	SMTP_server_address	Requis. Nom d'hôte et numéro de port du serveur SMTP de courrier sortant. Entrez ces informations dans le format suivant : <i>host_name:port_number</i>
-SMTPUserName -su	user_name	Facultatif. Nom d'utilisateur permettant l'authentification lors de l'envoi, si le serveur d'e-mail sortant l'exige.
-SMTPPassword -sp	password	Mot de passe utilisateur pour l'authentification lors de l'envoi si le serveur de courrier sortant le requiert. Vous pouvez définir le mot de passe avec l'option -sp ou la variable d'environnement INFA_PASSWORD. Si vous définissez le mot de passe avec les deux méthodes, la définition du mot de passe avec l'option -sp reçoit la priorité.
-SMTPSenderAddress -ss	sender_email_address	Facultatif. Adresse de courriel utilisée par le gestionnaire de service pour envoyer des courriels de notification. Si vous laissez ce champ vide, le gestionnaire de service utilise la valeur par défaut « Administrator@<host> » en tant qu'expéditeur.
-ResetSMTPUserNameAndPassword -re	reset_smtp_username_password	Facultatif. Configurez les paramètres pour le serveur de messagerie sortante SMTP afin de permettre à un utilisateur de s'abonner à des alertes.
-TLSEnabled -tls	is_tls_enabled	Facultatif. Indique que le serveur SMTP utilise le protocole TLS. S'il est défini sur True, entrez le numéro de port TLS comme propriété du port du serveur SMTP. Entrez True ou False. La valeur par défaut est False.

LIENS CONNEXES :

- [“AddAlertUser” à la page 352](#)

UpdateWSHubService

Met à jour un Hub de services Web dans le domaine.

La commande infacmd isp UpdateWSHubService utilise la syntaxe suivante :

```
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 ...]

```

Le tableau suivant décrit les options et arguments de la commande `infacmd isp UpdateWSHubService` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ServiceName -sn	service_name	Obligatoire. Nom du hub de services Web que vous souhaitez mettre à jour.
-NodeName -nn	node_name	Facultatif. Nom du nœud sur lequel s'exécute le processus du hub de services Web.
-ServiceOptions -so	option_name=value ...	Facultatif. Propriétés du service qui définissent le mode d'exécution du hub de services Web.

UpgradeGatewayNodeMetadata

Met à jour les métadonnées pour un nœud de passerelle sur la machine actuelle. Avant de mettre à jour le nœud de passerelle, exécutez la commande infacmd isp ShutDownNode pour arrêter le nœud.

La syntaxe de la commande UpgradeGatewayNodeMetadata est la suivante :

```
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]
```


Le tableau suivant décrit les options et les arguments de la commande *infasetup UpgradeGatewayNodeMetadata* :

Option	Description
-LogServiceDirectory -ld	Requis. Chemin du répertoire partagé utilisé par le gestionnaire de journaux pour stocker des fichiers d'événements de journal. Vérifiez que -ld ne correspond pas à la valeur--sld spécifiée ni ne la contient.
-SystemLogDirectory -sld	Facultatif. Chemin du répertoire pour stocker les fichiers journaux système. Vérifiez que -ld ne correspond pas à la valeur--sld spécifiée ni ne la contient. La valeur par défaut est <INFA_home>/logs.
-HttpsPort -hs	Facultatif. Numéro de port utilisé par le nœud pour la communication entre l'outil Administrator tool et le Gestionnaire de service. Définissez ce numéro de port si vous souhaitez configurer HTTPS pour un nœud. Pour désactiver le support HTTPS pour un nœud, initialisez ce numéro à zéro.
-KeystoreFile -kf	Facultatif. Le fichier keystore contenant les clés et les certificats est requis si vous utilisez le protocole de sécurité SSL.
-KeystorePass -kp	Facultatif. Mot de passe en texte brut du fichier keystore. Vous pouvez définir un mot de passe avec l'option -kp ou la variable d'environnement INFA_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -kp est prioritaire.
-DatabaseAddress -da	Obligatoire si vous n'utilisez pas l'option -DatabaseConnectionString (-cs). Nom et numéro du port de la machine hébergeant la base de données de configuration du domaine.
-DatabaseConnectionString -cs	Obligatoire si vous n'utilisez pas les options -DatabaseAddress (-da) et --DatabaseServiceName (-ds). Chaîne de connexion utilisée pour se connecter à la base de données de configuration du domaine. La chaîne de connexion doit inclure l'hôte de la base de données, le port de la base de données et le nom du service de base de données. Placez la chaîne de connexion entre guillemets.
-DatabaseUserName -du	Obligatoire si vous n'utilisez pas l'option -TrustedConnection (-tc). Compte de la base de données qui contient les informations de configuration du domaine.
-DatabasePassword -dp	Mot de passe de la base de données de configuration du domaine correspondant à l'utilisateur de la base de données. Si vous omettez cette option, <i>infasetup</i> utilisera le mot de passe spécifié dans la variable d'environnement INFA_DEFAULT_DATABASE_PASSWORD. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, vous devez entrer un mot de passe à l'aide de cette option.
-DatabaseType -dt	Requis. Type de base de données contenant les métadonnées de configuration du domaine. Les types de base de données sont les suivants : <ul style="list-style-type: none"> - db2 - oracle - mssqlserver - sybase - postgresql

Option	Description
-DatabaseServiceName -ds	Obligatoire si vous n'utilisez pas l'option -DatabaseConnectionString (-cs). Nom du service de base de données. Obligatoire pour les bases de données Oracle, IBM DB2 et Microsoft SQL Server. Entrez le SID pour Oracle, le nom du service pour IBM DB2 ou le nom de la base de données pour Microsoft SQL Server.
-Tablespace -ts	Obligatoire dans le cas d'une base de données IBM DB2. Nom de l'espace de table dans lequel se situent les tables de la base de données de configuration du domaine.
-SchemaName -sc	Facultatif. Nom du schéma Microsoft SQL Server. Entrez un nom de schéma si vous n'utilisez pas le schéma par défaut.
-TrustedConnection -tc	Facultatif. Connexion à la base de données Microsoft SQL Server via une connexion approuvée. L'authentification de confiance utilise les justificatifs d'identité de sécurité Windows de l'utilisateur en cours pour effectuer la connexion à Microsoft SQL Server.
-PreviousInfaHome -ph	Requis. Chemin du répertoire de base Informatica précédent.
-KeysDirectory -kd	Facultatif. Répertoire dans lequel sont stockés tous les fichiers Keytab et la clé de cryptage pour le domaine Informatica. La valeur par défaut est <InformaticaInstallationDir>/isp/config/keys.
-DatabaseTlsEnabled -dbtls	Facultatif. Indique si la base de données du domaine Informatica est sécurisée avec le protocole TLS ou SSL. Définissez cette option sur True pour la base de données sécurisée. La valeur par défaut est false. Si vous spécifiez l'option -dbtls sans valeur, le domaine Informatica utilise la communication sécurisée avec la base de données du domaine Informatica.
-DatabaseTruststorePassword -dbtp	Facultatif. Mot de passe du fichier truststore de la base de données sécurisée.
-DatabaseTruststoreLocation -dbtl	Facultatif. Chemin et nom du fichier truststore du nœud de passerelle.

validateFeature

Vérifie que la fonction spécifiée dans le fichier du plug-in est enregistrée dans le domaine.

La commande infacmd isp validateFeature utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd isp validateFeature :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-FeatureFilename -ff	feature_filename	Obligatoire. Chemin et nom du fichier XML du plug-in de la fonctionnalité enregistrée que vous souhaitez valider.

Version

Affiche la version de PowerCenter et les informations sur la marque commerciale et le copyright d'Informatica.

La commande Version utilise la syntaxe suivante :

```
infacmd version
```

CHAPITRE 22

Référence de commande infacmd Idm

Ce chapitre comprend les rubriques suivantes :

- [BackupContents, 793](#)
- [CreateService, 796](#)
- [ListServiceOptions, 802](#)
- [ListServiceProcessOptions, 803](#)
- [migrateContents, 805](#)
- [publishArchive, 807](#)
- [restoreContents, 809](#)
- [UpdateServiceOptions, 811](#)
- [UpdateServiceProcessOptions, 813](#)
- [mise à niveau, 815](#)

BackupContents

Vous pouvez exécuter cette commande en modes en ligne et hors ligne. Le mode hors ligne est défini par défaut. En mode en ligne ou hors ligne, le service de catalogue effectue une sauvegarde des données intermédiaires MongoDB, Solr, PostgreSQL et du scanner. Si le service de catalogue est compatible SSL, avant d'effectuer la sauvegarde en mode hors ligne, vous devez définir les variables d'environnement suivantes :

- INFA_KEYSTORE_PASSWORD chiffrée
- INFA_TRUSTSTORE_PASSWORD chiffrée
- INFA_TRUSTSTORE
- INFA_KEYSTORE

Remarque: Voir l'exemple de commande pour chiffrer le mot de passe : `$INFA_HOME/server/bin/pmpasswd <password>`

Par exemple :

- `export INFA_KEYSTORE_PASSWORD=hQDP8O8tfwxRSwbeANEptl4AIQqJcSj9ZMDkVK+9S+Y=`

- export INFA_TRUSTSTORE_PASSWORD=hx/nRWisSjnQ0zEGV3N7j1FCGF0m5RfisQxKTdf5f8Y=
- export INFA_TRUSTSTORE=/data/Informatica/LDM1040TO1050/services/shared/security/
- export INFA_KEYSTORE=/data/Informatica/LDM1040TO1050/services/shared/security

Avant d'exécuter cette commande, notez les points suivants :

- Si vous exécutez la commande en mode en ligne, vous devez vérifier que le service de catalogue est fonctionnel.
- Lorsque la sauvegarde en ligne est en cours, vous pouvez effectuer l'opération de lecture dans le service de catalogue.
- Si Solr est déployé sur plusieurs nœuds, le système de chemins de fichiers partagés du cluster doit être commun à tous les hôtes Solr, le système de chemins partagés du cluster doit être monté NFS et l'ID d'utilisateur de la passerelle doit être le même pour tous les hôtes Solr.
- La commande BackupContents requiert les variables d'environnement INFA_KEYSTORE et INFA_KEYSTORE_PASSWORD pour se connecter aux services Solr et MongoDB du service de cluster Informatica.

La syntaxe de la commande infacmd Idm BackupContents est la suivante :

```
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

[<-BackupMode|-mode> pass the mode in which backup is to be taken. Possible values are
OFFLINE or ONLINE. The default value is OFFLINE.]

[<-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.]
```

Le tableau suivant décrit les options et arguments d'infacmd Idm BackupContents :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	Password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de catalogue.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-OutputFilename -Of	Output_file_name	Obligatoire. Chemin d'accès complet et nom du fichier ZIP de sauvegarde sur la machine locale. La commande de sauvegarde crée le nom du fichier zip.

Option	Argument	Description
-BackupMode -mode	transmettre le mode dans lequel la sauvegarde doit être effectuée	Facultatif. Mode dans lequel vous voulez effectuer la sauvegarde. Spécifiez l'une des valeurs suivantes : - OFFLINE - ONLINE La valeur par défaut est OFFLINE.
-Force -fr	force	Facultatif. Pour forcer la sauvegarde lorsque le mode de sauvegarde est hors connexion. Force la sauvegarde et remplace l'actuelle.
-StoreType -st	Valeurs de types de magasins de données : - Asset - Orchestration - Search - Similarity	Facultatif. Indiquez le magasin de données requis ou la liste des magasins de données séparés par des virgules que vous souhaitez sauvegarder. En fonction des problèmes que vous souhaitez résoudre, vous pouvez sauvegarder les magasins de données requis au lieu d'effectuer une sauvegarde complète du catalogue. Vous pouvez sauvegarder les magasins de données suivants dans le catalogue : - Asset - Orchestration - Search - Similarity Vous devez sauvegarder les magasins de données Asset , Search et Similarity si vous souhaitez afficher les données après avoir restauré les données à partir de la sauvegarde. Remarque: Par défaut, la commande sauvegarde tous les magasins de données du catalogue. Pour plus d'informations, consultez les exemples ci-dessous : - Pour sauvegarder les magasins de données qui incluent Asset, Similarity, Search et Orchestration, ajoutez les arguments à l'option -st comme suit : -st Asset,Similarity, Search, and Orchestration.

CreateService

Crée un service de catalogue.

La syntaxe de la commande infacmd Idm CreateService est la suivante :

```
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]

```

Le tableau suivant décrit les options et les arguments de la commande `infacmd Idm CreateService` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-NodeName -nn	node_name	Requis. Nœud sur lequel vous voulez exécuter le service de catalogue.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de catalogue.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ModelRepositoryService -mrs	model_repository_service_name	Requis. Nom du service de référentiel modèle à associer au service de catalogue.
-MRSUserName -mrsun	model_repository_service_user_name	Obligatoire si vous spécifiez un service de référentiel modèle. Nom d'utilisateur pour la connexion au référentiel modèle. Si vous entrez un nom d'utilisateur qui contient un espace ou tout autre caractère non alphanumérique, placez-le entre guillemets.
-MRSPassword -mrspd	model_repository_service_user_password	Obligatoire si vous spécifiez un service de référentiel modèle. Mot de passe utilisateur pour le service de référentiel modèle.
-MRSSecurityDomain -mrssdn	model_repository_service_user_security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'administrateur.
-HttpPort -p	port_name	Requis. Un numéro de port HTTP unique utilisé pour chaque processus du service de catalogue. Le numéro de port par défaut est 9085.
-HttpsPort -sp	https_port_name	Requis si vous activez TLS (Transport Layer Security). Numéro de port de la connexion HTTPS.

Option	Argument	Description
-EnableTls -tls	enable_tls	Sélectionnez cette option pour activer TLS (Transport Layer Security).
-KeystoreFile -kf	keystore_file_location	Obligatoire si vous sélectionnez l'option Activer TLS (Transport Layer Security). Chemin d'accès et nom du fichier keystore. Le fichier keystore contient les clés et les certificats requis si vous utilisez le protocole de sécurité SSL avec Catalog Administrator.
-KeystorePassword -kp	keystore_password	Obligatoire si vous sélectionnez l'option Activer TLS (Transport Layer Security). Mot de passe du fichier keystore.
-SSLProtocol -sslp	ssl_protocol	Facultatif. Protocole Secure Sockets Layer à utiliser.
-InfaClusterServiceName -icsn	infa_cluster_service_name	Requis. Nom du service de cluster Informatica.
-isEmailEnabled -iee	is_email_enabled	Facultatif. Spécifiez la valeur True si vous souhaitez activer les notifications par courriel. La valeur par défaut est False.
-OtherOptions -oo	Autres options	Facultatif. Entrez la paire nom-valeur séparée par des espaces. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.
-BackupNodes -bn	node_name1,node_name2,...	Facultatif. Nœuds sur lesquels le service peut s'exécuter si le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.
-isNotifyChangeEmailEnabled -cne	is_notify_change_email_enabled	Facultatif. Spécifiez True pour activer les notifications de modification de la ressource. La valeur par défaut est False.
-EnableDataAssetAnalytics -ed	Activer le traitement analytique des actifs de données (True, False)	Requis. Spécifiez True pour activer le traitement analytique des actifs de données avec Enterprise Data Catalog. Si vous activez cette option, veillez à configurer les paramètres suivants : <ul style="list-style-type: none"> - DataAssetAnalyticsDBSelect - DataAssetAnalyticsDBUsername - DataAssetAnalyticsDBPassword - DataAssetAnalyticsDBURL

Option	Argument	Description
-DataAssetAnalyticsDBSelect -ddt	Sélectionnez la base de données pour le traitement analytique des actifs de données (ORACLE, SQLSERVER ou POSTGRESQL)	Requis si la valeur d'option <code>EnableDataAssetAnalytics</code> est définie sur True. Applique les bases de données suivantes : - Oracle - SQL Server - PostgreSQL
-DataAssetAnalyticsDBUsername -ddu	Nom d'utilisateur pour accéder à la base de données	Requis si la valeur d'option <code>EnableDataAssetAnalytics</code> est définie sur True. Spécifiez le nom d'utilisateur permettant d'accéder à la base de données pour le traitement analytique des actifs de données.
DataAssetAnalyticsDBPassword -ddp	Mot de passe configuré pour le nom d'utilisateur	Requis si la valeur d'option <code>EnableDataAssetAnalytics</code> est définie sur True. Spécifiez le mot de passe permettant d'accéder à la base de données pour le traitement analytique des actifs de données.
DataAssetAnalyticsDBURL -ddl	Chaîne de connexion de la base de données	Requis si la valeur d'option <code>EnableDataAssetAnalytics</code> est définie sur True. Spécifiez la chaîne de connexion de la base de données. Vérifiez que la chaîne de connexion commence par <code>'jdbc:informatica:'</code>
DataAssetAnalyticsDBSchema -dds	Nom du schéma de la base de données	Facultatif. Spécifiez le nom du schéma de la base de données. Applicable si vous aviez sélectionné SQL Server ou PostgreSQL comme type de base de données.
DataAssetAnalyticsSecureJDBCParameters -dsjdbcp	Paramètres de connexion JDBC sécurisés	Facultatif. Si la base de données du traitement analytique des actifs de données est sécurisée avec le protocole SSL, vous devez entrer les paramètres de base de données sécurisés. Entrez les paramètres au format de paires clé-valeur séparées par un point-virgule. Par exemple : <code>param1=value1;param2=value2</code>

ListServiceOptions

Répertorie les options du service de catalogue.

La syntaxe de la commande infacmd Idm ListServiceOptions est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd Idm ListServiceOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de catalogue.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>

ListServiceProcessOptions

Répertorie les options du processus de service pour le processus Catalog Administrator.

La syntaxe de la commande infacmd Idm ListServiceProcessOptions est la suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd Idm ListServiceProcessOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de catalogue.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-NodeName -nn	node_name	Requis. Obligatoire. Nom du nœud d'exécution du processus de service.

migrateContents

Migre le contenu. Fournissez le répertoire d'entrée à partir duquel vous souhaitez migrer ou vérifier le contenu. Exécutez la commande `migrateContents` lorsque le service de catalogue, le service de cluster Informatica et les magasins requis sont activés. Si le service de catalogue est compatible SSL, vous devez définir les variables d'environnement suivantes avant de migrer le contenu :

- Chiffrée. `INFA_KEYSTORE_PASSWORD`
- Chiffrée. `INFA_TRUSTSTORE_PASSWORD`
- `INFA_TRUSTSTORE`
- `INFA_KEYSTORE`

Remarque: Voir l'exemple de commande pour chiffrer le mot de passe : `$INFA_HOME/server/bin/pmpasswd <password>`

Par exemple :

- `export INFA_KEYSTORE_PASSWORD=hQDP808tfwxRSwbeANEptl4AIQqJcSj9ZMDkVK+9S+Y=`
- `export INFA_TRUSTSTORE_PASSWORD=hx/nRWisSjnQ0zEGV3N7j1FCGF0m5RfisQxKTdf5f8Y=`
- `export INFA_TRUSTSTORE=/data/Informatica/LDM1040TO1050/services/shared/security/`
- `export INFA_KEYSTORE=/data/Informatica/LDM1040TO1050/services/shared/security`

Remarque: Avant d'exécuter cette commande, notez les points suivants :

- La commande `migrateContents` requiert les variables d'environnement `INFA_KEYSTORE` et `INFA_KEYSTORE_PASSWORD` pour se connecter aux services Solr et MongoDB du service de cluster Informatica.
- Les utilisateurs administrateurs ou les utilisateurs qui font partie du groupe d'administrateurs peuvent exécuter la commande `migrateContents`.

La syntaxe de la commande `infacmd ldm migrateContents` est la suivante :

```
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.]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd Idm migrateContents` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de catalogue.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-InputDirectory -id	Répertoire d'entrée	Chemin d'accès complet au répertoire de sauvegarde. Par exemple, - /backup/export
-Resume	resume	Utilisez cette option pour reprendre la migration du contenu à partir du dernier point de contrôle disponible. Si la valeur est définie sur False, la migration commence depuis le début.
-Force	force	Utilisez cette option pour forcer le lancement d'un autre processus de migration en ignorant le verrou maintenu par le processus précédent.
-Verify	verify	Utilisez cette option pour vérifier les données restaurées une fois la migration terminée.

publishArchive

Crée une ressource en mode hors ligne et exécute l'analyse.

La syntaxe de la commande infacmd Idm publishArchive est la suivante :

```
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]

Le tableau suivant décrit les options et les arguments de la commande `infacmd Idm CreateService` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de catalogue.
-ResourceName -rn	Nom de la ressource	Requis. Nom de la ressource. Le nom ne peut pas dépasser 79 caractères, commencer ou se terminer par des espaces ou contenir des retours chariot, des tabulations ou les caractères suivants : <code>\ / * ? < > " \$</code>
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-DomainHost -dh	Nom d'hôte du domaine	Requis. Nom de la machine hôte où s'exécute le domaine.

Option	Argument	Description
-DomainPort -dp	Numéro de port du domaine	Obligatoire. Numéro de port du domaine.
-DomainSslEnabled -dse	is_Domain_SSL_Enabled	Facultatif. Spécifiez la valeur True pour activer le protocole SSL sur le domaine. La valeur par défaut est False.
-SslLocation -ts	-	Facultatif. Chemin d'accès au truststore.
-SslPassword -tsp	-	Facultatif. Mot de passe pour accéder au truststore.
-ArchiveFilePath -arf	-	Requis. Chemin d'accès au fichier d'archive des métadonnées.
-Verbose -v	Verbose	Facultatif. Affiche ou enregistre les informations de la purge en mode détaillé. Le mode détaillé fournit des informations détaillées sur les versions de l'objet, notamment le nom de référentiel, le nom de dossier, le numéro de version et l'état. Vous ne pouvez pas utiliser l'option -b avec -o et -p.
-WaitToCatalog -w	-	Facultatif. Attend la fin de l'ingestion de métadonnées dans le catalogue.
-Force -f	-	Facultatif. Crée ou met à jour la ressource.

restoreContents

Restaure la sauvegarde dans le mode que vous sélectionnez pour la commande BackupContents. Par exemple, si vous exécutez la commande BackupContents en mode hors ligne, la commande restoreContents est exécutée dans le même mode. Si le service de catalogue est compatible SSL, vous devez définir les variables d'environnement suivantes avant d'effectuer une restauration :

- Chiffrée. INFA_KEYSTORE_PASSWORD
- Chiffrée. INFA_TRUSTSTORE_PASSWORD
- INFA_TRUSTSTORE
- INFA_KEYSTORE

Remarque: Voir l'exemple de commande pour chiffrer le mot de passe : \$INFA_HOME/server/bin/pmpasswd <password>

Par exemple :

- export INFA_KEYSTORE_PASSWORD=hQDP808tfwxRSwbeANEptl4AIQqJcSj9ZMDkVK+9S+Y=
- export INFA_TRUSTSTORE_PASSWORD=hx/nRWisSjnQ0zEGV3N7j1FCGF0m5RfisQxKTdf5f8Y=
- export INFA_TRUSTSTORE=/data/Informatica/LDM1040TO1050/services/shared/security/

- export INFA_KEYSTORE=/data/Informatica/LDM1040TO1050/services/shared/security

Remarque: Avant d'exécuter cette commande, notez les points suivants :

- La commande restoreContents requiert les variables d'environnement INFA_KEYSTORE et INFA_KEYSTORE_PASSWORD pour se connecter aux services Solr et MongoDB du service de cluster Informatica.
- Vous ne devez pas utiliser la commande restoreContents pour restaurer la sauvegarde d'un nœud unique dans une configuration multinœud. Cette contrainte s'applique à l'option SEARCH store restore.

La syntaxe de la commande infacmd Idm restoreContents est la suivante :

```
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)]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd Idm restoreContents :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-ServiceName -sn	service_name	Requis. Nom du service de catalogue.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom de domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est Natif. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-InputFileName -if	input_file_name	Requis. Chemin d'accès complet au fichier .zip de sauvegarde sur l'hôte du service de catalogue.
-Force -fr	force	Facultatif. Utilisez cette option pour forcer le nettoyage du contenu existant du cluster Informatica où les données doivent être restaurées et restaurer les données de sauvegarde à partir de zéro.

UpdateServiceOptions

Met à jour les options du service de catalogue. Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

La syntaxe de la commande infacmd Idm UpdateServiceOptions est la suivante :

```
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,...]

Le tableau suivant décrit les options et les arguments de la commande `infacmd Idm UpdateServiceOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de catalogue.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-Options -o	options	<p>Facultatif. Entrez la paire nom-valeur séparée par des espaces. Vous pouvez mettre à jour les options suivantes relatives au traitement analytique des actifs de données :</p> <ul style="list-style-type: none"> - <code>DAARepository.EnableDataAssetAnalytics</code> : spécifiez <code>True</code> pour activer le traitement analytique des actifs de données. - <code>DAARepository.DataAssetAnalyticsDBSelect</code> : spécifiez l'une des bases de données suivantes : <ul style="list-style-type: none"> - Oracle - SQL Server - PostgreSQL - <code>DAARepository.DataAssetAnalyticsDBUsername</code> : spécifiez le nom d'utilisateur permettant d'accéder à la base de données du traitement analytique des actifs de données. - <code>DAARepository.DataAssetAnalyticsDBPassword</code> : spécifiez le mot de passe permettant d'accéder à la base de données du traitement analytique des actifs de données. - <code>DAARepository.DataAssetAnalyticsDBURL</code> : spécifiez la chaîne de connexion de la base de données. - <code>DAARepository.DataAssetAnalyticsDBSchema</code> : spécifiez le nom du schéma de la base de données. - <code>DAARepository.DataAssetAnalyticsSecureJDBCParameters</code> : spécifiez les paramètres de JDBC. Par exemple, <code>param1=value1;param2=value2</code>
-PrimaryNode -nn	node_name	Facultatif. Pour configurer la haute disponibilité d'Enterprise Data Catalog, spécifiez le nom du nœud principal.
-BackupNodes -bn	node_names	Facultatif. Pour configurer la haute disponibilité d'Enterprise Data Catalog, spécifiez une liste des noms de nœuds de sauvegarde séparés par une virgule.

UpdateServiceProcessOptions

Met à jour les options de processus de service de catalogue. Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

La syntaxe de la commande `infacmd Idm UpdateServiceProcessOptions` est la suivante :

```
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

Le tableau suivant décrit les options et arguments d'infacmd Idm UpdateServiceProcessOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-NodeName -nn	node_name	Requis. Nom du nœud d'exécution du processus de service.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de catalogue.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Options -o	options	Requis. Entrez la paire nom-valeur séparée par des espaces.

mise à niveau

Met à niveau le service de catalogue.

La syntaxe de la commande infacmd Idm upgrade est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd Idm upgrade :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de catalogue.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

CHAPITRE 23

Référence de commande infacmd mas

Ce chapitre comprend les rubriques suivantes :

- [CreateService, 817](#)
- [ListServiceOptions, 821](#)
- [ListServiceProcessOptions, 823](#)
- [UpdateServiceOptions, 825](#)
- [UpdateServiceProcessOptions, 828](#)

CreateService

Crée un service d'accès aux métadonnées. Le service d'accès aux métadonnées est un service d'application qui permet à l'outil Developer tool d'accéder aux informations de connexion Hadoop pour l'importation et l'aperçu des métadonnées.

La syntaxe de la commande infacmd mas CreateService est la suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de d'infacmd mas CreateService :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-NodeName -nn	node_name	Nœud où le service d'accès aux métadonnées s'exécute. Vous pouvez exécuter le service d'intégration de données uniquement sur un nœud.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-ServiceName -sn	service_name	Requis. Nom du service d'accès aux métadonnées. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 230 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "
-HTTPProtocolType -hp	http_protocol_type	Protocole de sécurité que le service d'accès aux métadonnées utilise. Entrez l'une des valeurs suivantes : - HTTP. Les demandes effectuées auprès du service doivent utiliser une URL HTTP. - HTTPS. Les demandes effectuées auprès du service doivent utiliser une URL HTTPS. Lorsque vous définissez le type de protocole HTTP sur HTTPS, vous devez activer TLS (Transport Layer Security) pour le service. La valeur par défaut est HTTP.
-HTTPPort -pt	http_port	Obligatoire si vous ne spécifiez pas de port HTTPS. Numéro de port HTTP unique utilisé pour chaque processus de service d'accès aux métadonnées. Après avoir créé le service, vous pouvez définir des numéros de port différents pour chaque processus de service d'accès aux métadonnées. La valeur par défaut est 7080. Le service d'accès aux métadonnées utilise des numéros de ports consécutifs pour se connecter à plusieurs distributions Hadoop.
-HTTPSPort -spt	https_port	Obligatoire si vous ne spécifiez pas de port HTTP. Numéro de port HTTPS unique utilisé pour chaque processus de service d'accès aux métadonnées. Après avoir créé le service, vous pouvez définir des numéros de port différents pour chaque processus de service d'accès aux métadonnées. Le service d'accès aux métadonnées utilise des numéros de ports consécutifs pour se connecter à plusieurs distributions Hadoop.
-HadoopServicePrincipalName -hpn	hadoop_spn	Nom de principal de service (SPN) du service d'accès aux métadonnées pour se connecter à un cluster Hadoop utilisant l'authentification Kerberos. Ne s'applique pas à la distribution MapR.
-HadoopKeyTab -hkt	keytab_file_path	Chemin du fichier keytab de Kerberos sur la machine sur laquelle le service d'accès aux métadonnées s'exécute. Ne s'applique pas à la distribution MapR.
-ServiceDescription -sd	service_description	Facultatif. Description du service.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-FolderPath -fp	full_folder_path	Facultatif. Chemin d'accès complet, sans le nom de domaine, du dossier dans lequel vous souhaitez créer le service d'accès aux métadonnées. Doit être au format suivant : /parent_folder/child_folder La valeur par défaut est « / » (le domaine).
-BackupNodes -bn	node_name1,node_name 2,...	Facultatif. Nœuds sur lesquels le service peut s'exécuter si le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.
-KeystoreFile -kf	keystore_file_location	Chemin et nom du fichier keystore contenant les clés et les certificats requis si vous utilisez le protocole HTTPS pour le service d'accès aux métadonnées. Vous pouvez créer un fichier keystore à l'aide de keytool. keytool est un utilitaire qui génère et stocke des paires de clés privées ou publiques et les certificats associés dans un fichier keystore. Vous pouvez utiliser le certificat auto-signé ou un certificat signé par une autorité de certification.
-KeystorePassword -kp	keystore_password	Mot de passe pour le fichier keystore
-TruststoreFile -tf	trust_store_file	Requis lorsque le domaine est compatible avec le protocole SSL. Emplacement du fichier truststore du domaine dans le cluster.
-TruststorePassword -tp	trust_store_password	Requis lorsque le domaine est compatible avec le protocole SSL. Mot de passe du domaine truststore.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-SSLProtocol -sp	ssl_protocol	Facultatif. Protocole Secure Sockets Layer à utiliser.
-HadoopImpersonationUser -hu	hadoop_impersonation_user	Facultatif. Entrez un nom d'utilisateur pour que le service d'accès aux métadonnées emprunte l'identité lorsqu'il se connecte à l'environnement Hadoop.
-loggedInUserAsImpersonationUser -uiu	use_logged_in_user_as_proxy	Requis si la grappe Hadoop utilise l'authentification Kerberos. Utilisateur d'emprunt d'identité Hadoop. Le nom d'utilisateur avec lequel le service d'accès aux métadonnées emprunte l'identité pour importer des métadonnées à partir de l'environnement Hadoop au moment de la conception.
-enableOSProfile -osp	enable_OS_profile	Indique que le service d'accès aux métadonnées peut utiliser les profils du système d'exploitation pour l'aperçu des métadonnées. La valeur par défaut est false.

ListServiceOptions

Répertorie les propriétés d'un service d'accès aux métadonnées.

La syntaxe de la commande infacmd mas ListServiceOptions est la suivante :

```
ListServiceOptions
<-DomainName|-dn> DomainName
<-UserName|-un> Username
<-Password|-pd> Password
<-ServiceName|-sn> ServiceName
[<-SecurityDomain|-sdn> SecurityDomain]
```

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

Le tableau suivant décrit les options et arguments d'infacmd mas ListServiceOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'accès aux métadonnées.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

ListServiceProcessOptions

Répertorie les propriétés d'un processus de service d'accès aux métadonnées.

La syntaxe de la commande infacmd mas ListServiceProcessOptions est la suivante :

```
ListServiceProcessOptions
<-DomainName|-dn> DomainName
<-NodeName|-nn> NodeName
<-UserName|-un> Username
<-Password|-pd> Password
<-ServiceName|-sn> ServiceName
[<-SecurityDomain|-sdn> SecurityDomain]
[<-ResilienceTimeout|-re> ResilienceTimeout]
```

Le tableau suivant décrit les options et arguments d'infacmd mas ListServiceProcessOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-NodeName -nn	node_name	Obligatoire. Nom de nœud où le processus de service s'exécute.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'accès aux métadonnées.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

UpdateServiceOptions

Met à jour les propriétés du service d'accès aux métadonnées. Pour afficher les propriétés actuelles, exécutez la commande `infacmd mas ListServiceOptions`.

Vous pouvez modifier les propriétés pendant l'exécution du service, mais vous devez redémarrer celui-ci pour que les modifications entrent en vigueur.

La syntaxe de la commande `infacmd mas UpdateServiceOptions` est la suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd mas UpdateServiceOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'accès aux métadonnées dans lequel l'application est déployée.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-Options -o	options	Facultatif. Entrez chaque option en la séparant par un espace. Pour afficher les options, exécutez la commande <code>infacmd mas ListServiceOptions</code> .
-PrimaryNode -nn	node_name	Entrez le nœud où le service d'accès aux métadonnées s'exécutera. Le service d'accès aux métadonnées peut s'exécuter uniquement sur un nœud.
-BackupNodes -bn	node_name1,node_name2,.. ..	Facultatif. Nœuds sur lesquels le service peut s'exécuter si le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.
-SearchIndexRoot -si	search_index_root	Facultatif. Change le répertoire de l'index de recherche. Entrez le chemin complet du répertoire. Le répertoire par défaut est le répertoire d'installation Informatica.

Options du service d'accès aux métadonnées

Utilisez les options du service d'accès aux métadonnées avec la commande `infacmd mas UpdateServiceOptions`.

Entrez les options du service d'accès aux métadonnées au format suivant :

```
... -o option_type.option_name=value
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options du service d'accès aux métadonnées :

Option	Description
ExecutionContextOptions.HadoopDistribution	Le répertoire de distribution Hadoop sur le nœud du service d'accès aux métadonnées. Le contenu du répertoire de distribution Hadoop du service d'accès aux métadonnées doit être identique à celui du répertoire de distribution Hadoop sur les nœuds de données. Entrez <code><Informatica Installation directory>/Informatica/services/shared/hadoop/[Hadoop_distribution_name]</code> .
HttpConfigurationOptions.HTTPProtocolType	<p>Protocole de sécurité que le service d'accès aux métadonnées utilise. Entrez l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> - HTTP. Les demandes effectuées auprès du service doivent utiliser une URL HTTP. - HTTPS. Les demandes effectuées auprès du service doivent utiliser une URL HTTPS. <p>Lorsque vous définissez le type de protocole HTTP sur HTTPS, vous devez activer TLS (Transport Layer Security) pour le service. La valeur par défaut est HTTP.</p>
MASProperties.EnableOSProfile	Indicateur pour spécifier si le service d'accès aux métadonnées peut utiliser les profils du système d'exploitation pour l'aperçu des métadonnées. La valeur par défaut est false.

Option	Description
MASProperties.HadoopKeytab	Chemin du fichier keytab de Kerberos sur la machine sur laquelle le service d'accès aux métadonnées s'exécute. Ne s'applique pas à la distribution MapR.
MASProperties.HadoopPrincipal	Nom de principal de service (SPN) du service d'accès aux métadonnées pour se connecter à un cluster Hadoop utilisant l'authentification Kerberos. Ne s'applique pas à la distribution MapR.
MASProperties.LoggedInUserAsImperUser	Obligatoire si le cluster Hadoop utilise l'authentification Kerberos.

UpdateServiceProcessOptions

Met à jour les propriétés d'un processus de service d'accès aux métadonnées. Pour afficher les propriétés actuelles, exécutez la commande `infacmd mas ListServiceProcessOptions`.

Entrez les options en utilisant le format suivant :

```
... -o option_name=value option_name=value ...
```

Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

La syntaxe de la commande `infacmd mas UpdateServiceProcessOptions` est la suivante :

```
UpdateServiceProcessOptions
<-DomainName|-dn> DomainName
<-NodeName|-nn> NodeName
<-UserName|-un> Username
<-Password|-pd> Password
<-ServiceName|-sn> ServiceName
[<-SecurityDomain|-sdn> SecurityDomain]
[<-ResilienceTimeout|-re> ResilienceTimeout]
```

Le tableau suivant décrit les options et arguments d'`infacmd mas UpdateServiceProcessOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
NodeName -nn	node_name	Obligatoire. Nœud où le service d'accès aux métadonnées s'exécute.

Option	Argument	Description
-UserName -un	user_name	<p>Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>
-Password -pd	password	<p>Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p>
-ServiceName -sn	service_name	Obligatoire. Nom du service d'accès aux métadonnées.
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>

Options de processus de service d'accès aux métadonnées

Utilisez les options de processus de service d'accès aux métadonnées avec la commande `infacmd mas UpdateServiceProcessOptions`.

Entrez les options de processus de service d'accès aux métadonnées au format suivant :

```
... -o option_type.option_name=value
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de processus de service d'accès aux métadonnées :

Option	Description
GeneralOptions.JVMOptions	Options de ligne de commande de la machine virtuelle Java (JVM) pour l'exécution de programmes Java. Lorsque vous configurez les options JVM, vous devez définir le chemin de classe, ainsi que la mémoire minimale et maximale Java SDK.
HttpConfigurationOptions.KeyStoreFile	Chemin et nom du fichier keystore contenant les clés et les certificats requis si vous utilisez le protocole HTTPS pour le service d'accès aux métadonnées. Vous pouvez créer un fichier keystore à l'aide de <code>keytool</code> . <code>keytool</code> est un utilitaire qui génère et stocke des paires de clés privées ou publiques et les certificats associés dans un fichier keystore. Vous pouvez utiliser le certificat auto-signé ou un certificat signé par une autorité de certification.
HttpConfigurationOptions.KeyStorePassword	Mot de passe pour le fichier keystore
HttpConfigurationOptions.MaxBacklogRequests	Nombre maximal de connexions HTTP ou HTTPS pouvant patienter dans une file d'attente pour ce processus de service d'accès aux métadonnées. Par défaut 100.
HttpConfigurationOptions.MaxConcurrentRequests	Nombre maximal de connexions HTTP ou HTTPS pouvant être établies vers ce processus de service d'accès aux métadonnées. La valeur minimale est 4. La valeur par défaut est 200.
HttpConfigurationOptions.SSLProtocol	Protocole Secure Sockets Layer à utiliser. La valeur par défaut est TLS.
HttpConfigurationOptions.TrustStoreFile	Chemin et nom du fichier truststore contenant les certificats d'authentification approuvés pour le service d'accès aux métadonnées.
HttpConfigurationOptions.TrustStorePassword	Mot de passe pour le fichier truststore.

CHAPITRE 24

Référence de commande infacmd mi

Ce chapitre comprend les rubriques suivantes :

- [abortRun, 831](#)
- [clearSamlConfig, 832](#)
- [createService, 833](#)
- [deploySpec, 836](#)
- [exportSpec, 838](#)
- [extendedRunStats, 839](#)
- [getSpecRunStats, 841](#)
- [listSpecRuns, 842](#)
- [listSpecs, 843](#)
- [restartMapping, 844](#)
- [runSpec, 845](#)
- [updateSamlConfig, 847](#)

abortRun

Abandonne les tâches de mappage d'ingestion dans une instance d'exécution d'une spécification Ingestion de masse. Lorsque vous abandonnez les tâches de mappage d'ingestion, la commande abandonne les mappages qui effectuent les tâches d'ingestion pour toutes les tables source en cours d'exécution ou en file d'attente. La commande n'abandonne pas les mappages des tâches d'ingestion terminées.

Pour abandonner les tâches de mappage d'ingestion, vous devez spécifier un RunID. Pour rechercher le RunID d'une instance d'exécution, répertoriez les instances d'exécution de spécification en utilisant infacmd mi listSpecRuns.

La syntaxe de la commande infacmd mi abortRun est la suivante :

```
abortRun

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]
```

```
<-ServiceName|-sn> service_name
```

```
<-runID|-rid> run_id
```

Le tableau suivant décrit les options et arguments d'infacmd mi abortRun :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Password -pd	mot de passe	Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Facultatif. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. La valeur par défaut est Native.
-ServiceName -sn	service_name	Requis. Nom du service d'ingestion de masse qui gère la spécification d'ingestion de masse.
-runID -rid	run_id	Obligatoire. Exécutez le numéro d'identificateur, ou l'ID d'exécution, de l'instance d'exécution de la spécification d'ingestion de masse. Pour rechercher le RunID d'une instance d'exécution, répertoriez les instances d'exécution de spécification en utilisant infacmd mi listSpecRuns.

clearSamlConfig

Efface la configuration SAML du service d'ingestion de masse pour la réinitialiser sur les valeurs par défaut.

La syntaxe de la commande infacmd mi clearSamlConfig est la suivante :

```
clearSamlConfig
```

```
<-DomainName|-dn> domain_name
```

```
<-UserName|-un> user_name
```

```
<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]
```

```
<-ServiceName|-sn> service_name
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd mi clearSamlConfig` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Facultatif. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. La valeur par défaut est Native.
-ServiceName -sn	service_name	Requis. Nom du service d'ingestion de masse qui gère la spécification d'ingestion de masse.

createService

Crée un service d'ingestion de masse. Lorsque vous créez le service d'ingestion de masse, vous devez spécifier un service de référentiel modèle. Le service d'ingestion de masse est désactivé par défaut. Pour activer le service d'ingestion de masse, utilisez `infacmd isp enableService`.

La syntaxe de la commande `infacmd mi createService` est la suivante :

```
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]

```

Le tableau suivant décrit les options et arguments d'infacmd mi createService :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Password -pd	mot de passe	Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Facultatif. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.
-Gateway -hp	gateway_host1:port gateway_host2:port	Requis si les informations de connectivité de passerelle du fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'ingestion de masse. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 230 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "
-HttpPort -http	http_port	Obligatoire si vous ne spécifiez pas de port HTTPS. Numéro de port HTTP unique utilisé pour chaque processus du service d'ingestion de masse. Après avoir créé le service, vous pouvez définir des numéros de port différents pour chaque processus du service d'ingestion de masse. La valeur par défaut est 9050. Remarque: Vous ne pouvez pas spécifier à la fois un port HTTP et un port HTTPS.
-HttpsPort -https	https_port	Obligatoire si vous ne spécifiez pas de port HTTP. Numéro de port HTTPS unique utilisé pour chaque processus du service d'ingestion de masse. Après avoir créé le service, vous pouvez définir des numéros de port différents pour chaque processus de service d'ingestion de masse. Remarque: Vous ne pouvez pas spécifier à la fois un port HTTP et un port HTTPS.

Option	Argument	Description
-KeystoreFile -kf	keystore_file_location	Obligatoire si vous spécifiez un port HTTPS. Chemin et nom du fichier keystore contenant les clés et les certificats requis si vous utilisez le protocole HTTPS pour le service d'ingestion de masse. Vous pouvez créer un fichier keystore à l'aide de keytool. keytool est un utilitaire qui génère et stocke des paires de clés privées ou publiques et les certificats associés dans un fichier keystore. Vous pouvez utiliser le certificat auto-signé ou un certificat signé par une autorité de certification.
-KeystorePassword -kp	keystore_password	Obligatoire si vous spécifiez un port HTTPS. Mot de passe du fichier keystore.
-LicenseName -ln	license_name	Requis. Nom de la licence à attribuer au service d'ingestion de masse. Pour appliquer les modifications, redémarrez le service d'ingestion de masse.
-FolderPath -fp	full_folder_path	Facultatif. Chemin d'accès complet, sans le nom de domaine, du dossier dans lequel vous souhaitez créer le service d'ingestion de masse. Doit être au format suivant : <i>/parent_folder/child_folder</i> La valeur par défaut est le domaine : /
-NodeName -nn	node_name	Requis. Nœud où le service d'ingestion de masse s'exécute.
-RepositoryService -rs	Repository_service_name	Obligatoire. Service de référentiel modèle qui stocke les métadonnées pour les spécifications d'ingestion de masse.
-RepositoryUser -Ru	Repository_user	Facultatif. Nom d'utilisateur permettant l'accès au service de référentiel modèle.
-RepositoryPassword -Rp	Repository_password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour l'accès au service de référentiel modèle.
-RepositoryUserSecurityDomain -Rsdn	Repository_user_security_domain	Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur du référentiel modèle.

deploySpec

Déploie une spécification d'ingestion de masse. Lorsque vous déployez la spécification, vous devez spécifier le service d'intégration de données et la connexion Hadoop. Vous devez déployer une spécification

d'ingestion de masse avant de pouvoir l'exécuter. Après avoir déployé la spécification, exécutez-la à l'aide de infacmd mi runSpec.

La syntaxe de la commande infacmd mi deploySpec est la suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd mi deploySpec :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Password -pd	mot de passe	Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Facultatif. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. La valeur par défaut est Native.
-ServiceName -sn	service_name	Requis. Nom du service d'ingestion de masse qui gère la spécification d'ingestion de masse.
-DISServiceName -dis	data_integration_service	Obligatoire. Nom du service d'intégration de données dans lequel vous voulez déployer la spécification d'ingestion de masse.

Option	Argument	Description
-MISpecName -Spec	Mi_spec_name	Obligatoire. Nom de la spécification d'ingestion de masse à déployer dans le service d'intégration de données.
-HadoopConnection -hc	Hadoop_connection	Obligatoire. La connexion Hadoop que le service d'intégration de données utilise pour transmettre (en push) la spécification d'ingestion de masse à l'environnement Hadoop.

exportSpec

Exporte la spécification d'ingestion de masse dans un fichier d'archive d'application. Lorsque vous exportez la spécification, vous devez spécifier le répertoire dans lequel vous souhaitez enregistrer le fichier. Vous pouvez déployer le fichier d'archive d'application dans un service d'intégration de données en utilisant infacmd dis DeployApplication.

La syntaxe de la commande infacmd mi exportSpec est la suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd mi exportSpec :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Password -pd	Password	Obligatoire. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Facultatif. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. La valeur par défaut est Native.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'ingestion de masse qui gère la spécification d'ingestion de masse.
-MISpecName -Spec	Mi_spec_name	Obligatoire. Nom de la spécification d'ingestion de masse à exporter.
-Directory -Dir	Dir_path	Obligatoire. Le répertoire d'enregistrement du fichier d'archive d'application.
-HadoopConnection -hc	Hadoop_connection	Obligatoire. La connexion Hadoop que le service d'intégration de données utilisera pour exécuter la tâche d'ingestion de masse lorsque vous importez le fichier d'archive d'application et que vous exécutez l'application. Vous devez spécifier la connexion Hadoop car celle-ci n'est pas permanente pour la spécification d'ingestion de masse tandis que la spécification est stockée dans le référentiel modèle.

extendedRunStats

Obtient les statistiques d'ingestion étendues pour une table source spécifique dans la spécification d'ingestion de masse déployée. Pour obtenir les statistiques étendues, vous devez spécifier le RunID de la spécification d'ingestion de masse, le nom de la table source et le type de mappage.

Les statistiques étendues rapportent les statistiques d'ingestion des lignes de tableau ingérées depuis la source et les statistiques d'ingestion pour les lignes de tableau ingérées dans la cible. Les statistiques répertorient le nombre de lignes qui ont été ingérées et le nombre de lignes qui contiennent des erreurs.

Si l'instance d'exécution utilise une charge incrémentielle, les statistiques étendues rapportent également la clé incrémentielle et la valeur de début. La clé incrémentielle est le nom de la colonne que le moteur Spark a utilisé pour récupérer les données incrémentielles dans la table source. La valeur de départ est celle que le moteur Spark a utilisée pour démarrer l'ingestion des données incrémentielles.

La syntaxe de la commande infacmd mi extendedRunStats est la suivante :

```
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

```

Le tableau suivant décrit les options et arguments d'infacmd mi extendedRunStats :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Password -pd	mot de passe	Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Facultatif. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. La valeur par défaut est Native.
-ServiceName -sn	service_name	Requis. Nom du service d'ingestion de masse qui gère la spécification d'ingestion de masse associée à la tâche de mappage de l'ingestion.
-RunID -rid	run_id	Obligatoire. Exécutez le numéro d'identificateur, ou l'ID d'exécution, de l'instance d'exécution de la spécification d'ingestion de masse. Pour rechercher le RunID d'une instance d'exécution, répertoriez les instances d'exécution de spécification en utilisant la commande infacmd mi listSpecRuns.
-SourceName -srcName	source_name	Obligatoire. Nom de la table source dans l'instance d'exécution de la spécification de l'ingestion de masse. Pour rechercher le nom de la table source, obtenez les statistiques de l'exécution de l'ingestion à l'aide de la commande infacmd mi getSpecRunStats.
-MappingTp -Mtp	Mapping_type	Obligatoire. Le type de mappage correspond au moteur d'exécution qui exécute la tâche de mappage de l'ingestion pour la table source. Pour rechercher le type de mappage, obtenez les statistiques de l'exécution de l'ingestion à l'aide de la commande infacmd mi getSpecRunStats.

getSpecRunStats

Obtient les statistiques d'exécution détaillées pour une spécification d'ingestion de masse déployée. Pour obtenir les statistiques, vous devez spécifier un RunID. Pour rechercher le RunID d'une instance d'exécution, répertoriez les instances d'exécution de spécification en utilisant infacmd mi listSpecRuns.

Les statistiques d'exécution détaillées rapportent le JobID pour chaque tâche de mappage de l'ingestion dans la spécification d'ingestion de masse déployée, le nom de la table source que chaque tâche de mappage ingère, l'heure de début de l'exécution, l'heure de fin, le moteur d'exécution qui exécute la tâche de mappage, et le statut de la tâche. JobID est l'ID de la tâche de mappage de l'ingestion qui ingère la table source. Il est possible que le statut indique Terminé, En échec, Annulé, En cours d'exécution, Abandonné, En file d'attente ou Inconnu.

La syntaxe de la commande infacmd mi getSpecRunStats est la suivante :

```
getSpecRunStats

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-ServiceName|-sn> service_name

<-runID|-rid> run_id
```

Le tableau suivant décrit les options et arguments d'infacmd mi getSpecRunStats :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Password -pd	password	Obligatoire. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Facultatif. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. La valeur par défaut est Native.

Option	Argument	Description
-ServiceName -sn	service_name	Obligatoire. Nom du service d'ingestion de masse qui gère la spécification d'ingestion de masse.
-runID -rid	run_id	Obligatoire. Exécutez le numéro d'identificateur, ou l'ID d'exécution, de l'instance d'exécution de la spécification d'ingestion de masse. Pour rechercher le RunID d'une instance d'exécution, répertoriez les instances d'exécution de spécification en utilisant infacmd mi listSpecRuns.

listSpecRuns

Répertorie les instances d'exécution d'une spécification d'ingestion de masse déployée. Chaque instance d'exécution est définie par un RunID. Lorsque vous répertoriez les instances d'exécution, vous devez spécifier le service d'ingestion de masse.

Les statistiques d'exécution détaillées rapportent le RunID pour chaque instance d'exécution de spécification, le type de charge, l'heure de début de l'instance d'exécution, le service d'intégration de données où la spécification d'ingestion de masse est déployée, l'utilisateur qui a démarré l'exécution et le statut de tâche pour chaque instance d'exécution. Il est possible que le statut indique Terminé, En échec, Annulé, En cours d'exécution, En file d'attente ou Inconnu.

La syntaxe de la commande infacmd mi listSpecRuns est la suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd mi listSpecRuns :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.

Option	Argument	Description
-Password -pd	mot de passe	Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Facultatif. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. La valeur par défaut est Native.
-ServiceName -sn	service_name	Requis. Nom du service d'ingestion de masse qui gère la spécification d'ingestion de masse.
-MISpecName -Spec	Mi_spec_name	Obligatoire. Nom de la spécification d'ingestion de masse.

listSpecs

Répertorie les spécifications d'ingestion de masse. Lorsque vous répertoriez les spécifications, vous devez spécifier le service d'ingestion de masse.

La syntaxe de la commande infacmd mi listSpecs est la suivante :

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

Le tableau suivant décrit les options et arguments d'infacmd mi listSpecs :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.

Option	Argument	Description
-Password -pd	password	Obligatoire. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Facultatif. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. La valeur par défaut est Native.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'ingestion de masse qui gère les spécifications d'ingestion de masse.

restartMapping

Redémarre les tâches de mappage de l'ingestion dans une spécification d'ingestion de masse. Spécifiez la liste des tables sources à redémarrer. Vous devez spécifier le service d'ingestion de masse et le RunID pour l'instance d'exécution de la spécification d'ingestion de masse. Vous pouvez également spécifier si vous souhaitez redémarrer uniquement les tables sources en échec.

La syntaxe de la commande infacmd mi restartMapping est la suivante :

```
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]
```


Le tableau suivant décrit les options et arguments d'infacmd mi restartMapping :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Password -pd	password	Obligatoire. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Facultatif. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. La valeur par défaut est Native.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'ingestion de masse qui gère l'ingestion des tables sources.
-runID -rid	run_id	Obligatoire. Numéro d'identificateur d'exécution (ID d'exécution) de l'instance d'exécution de la spécification d'ingestion de masse.
-SourceList -srcList	comma_separated_source_list	Obligatoire. La liste des tables sources à redémarrer. Séparez chaque table source par une virgule.
-OnlyFailed -failed	true false	Facultatif. Entrez True pour redémarrer uniquement les tables sources qui n'ont pas été ingérées. Entrez False pour redémarrer toutes les tables sources.

runSpec

Exécute une spécification d'ingestion de masse qui est déployée dans un service d'intégration de données. Pour pouvoir exécuter une spécification, vous devez déployer la spécification en utilisant infacmd mi deploySpec.

La syntaxe de la commande infacmd mi runSpec est la suivante :

```
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]

```

Le tableau suivant décrit les options et arguments d'infacmd mi runSpec :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Password -pd	mot de passe	Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Facultatif. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. La valeur par défaut est Native.
-ServiceName -sn	service_name	Requis. Nom du service d'ingestion de masse qui gère la spécification d'ingestion de masse.
-MISpecName -Spec	Mi_spec_name	Obligatoire. Nom de la spécification d'ingestion de masse qui est déployée dans le service d'intégration de données.

Option	Argument	Description
-LoadType -lt	load_type	Facultatif. Type de charge pour ingérer les données dans la spécification d'ingestion de masse. Utilisez <code>full</code> ou <code>incremental</code> . La valeur par défaut est <code>full</code> . Si la charge incrémentielle n'est pas activée dans la spécification d'ingestion de masse, vous ne pouvez pas utiliser ce type de charge pour l'ingestion des données.
-DISServiceName -dis	data_integration_service	Obligatoire. Nom du service d'intégration de données où la spécification d'ingestion de masse est déployée.
-OperatingSystemProfile -osp	operating_system_profile_name	Facultatif. Nom du profil de système d'exploitation configuré pour le service d'intégration de données.

updateSamlConfig

Met à jour la configuration SAML du service d'ingestion de masse. Vous pouvez configurer l'URL du fournisseur d'identité, l'ID de fournisseur de service, la tolérance de variation d'horloge et l'alias de certificat de signature d'assertion.

La syntaxe de la commande `infacmd mi updateSamlConfig` est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd mi updateSamlConfig` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Facultatif. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. La valeur par défaut est Native.
-ServiceName -sn	service_name	Requis. Nom du service d'ingestion de masse qui gère la spécification d'ingestion de masse.
-idpUrl -iu	url_fournisseur_identité	Facultatif. Spécifiez l'URL du fournisseur d'identité du domaine. Vous devez spécifier la chaîne complète de l'URL.
-ServiceProviderId -spid	service_provider_id	Facultatif. Nom d'approbation de la partie de confiance ou identificateur de fournisseur de services pour le domaine, tel que défini dans le fournisseur d'identité. Si vous avez spécifié « Informatica » comme nom de tiers de confiance dans AD FS, vous n'avez pas besoin de spécifier une valeur.

Option	Argument	Description
-ClockSkewTolerance -cst	clock_skew_tolerance_in_seconds	<p>Facultatif. Différence temporelle autorisée entre l'horloge système du fournisseur d'identité et celle du nœud principal de passerelle.</p> <p>La durée de vie des jetons SAML émis par le fournisseur d'identité est définie selon l'horloge système de l'hôte du fournisseur d'identité. La durée de vie est valide si l'heure de début ou l'heure de fin définie dans le jeton est comprise dans le nombre de secondes spécifié de l'horloge système du nœud principal de passerelle.</p> <p>Les valeurs doivent être comprises entre 0 et 600 secondes. La valeur par défaut est 120 secondes.</p>
-AssertionSigningCertificateAlias -asca	idp_assertion_signing_certificate_alias	<p>Facultatif. Nom d'alias spécifié lors de l'importation du certificat de signature d'assertion du fournisseur d'identité dans le fichier truststore utilisé pour l'authentification SAML.</p> <p>Si vous modifiez le nom de l'alias, importez le certificat correspondant dans le fichier truststore de chaque nœud de passerelle, puis redémarrez le nœud.</p>

CHAPITRE 25

Référence de commande infacmd mrs

Ce chapitre comprend les rubriques suivantes :

- [BackupContents, 851](#)
- [CheckInObject, 853](#)
- [CreateContents, 855](#)
- [CreateFolder, 857](#)
- [CreateProject, 858](#)
- [CreateService, 860](#)
- [DeleteContents, 864](#)
- [DeleteFolder, 866](#)
- [DeleteProject, 868](#)
- [disableMappingValidationEnvironment, 870](#)
- [enableMappingValidationEnvironment, 872](#)
- [ListBackupFiles, 875](#)
- [ListCheckedOutObjects, 876](#)
- [listFolders, 878](#)
- [ListLockedObjects, 880](#)
- [listMappingEngines, 882](#)
- [listPermissionOnProject, 884](#)
- [ListProjects, 886](#)
- [ListServiceOptions, 888](#)
- [ListServiceProcessOptions, 889](#)
- [ManageGroupPermissionOnProject, 891](#)
- [ManageUserPermissionOnProject, 893](#)
- [PopulateVCS, 895](#)
- [ReassignCheckedOutObject, 896](#)
- [rebuildDependencyGraph, 898](#)
- [RenameFolder, 900](#)
- [replaceMappingHadoopRuntimeConnections, 901](#)
- [RestoreContents, 903](#)

- [UndoCheckout, 905](#)
- [setMappingExecutionEnvironment, 907](#)
- [UndoCheckout, 909](#)
- [UnlockObject, 911](#)
- [UpdateServiceOptions, 913](#)
- [UpdateServiceProcessOptions, 920](#)
- [UpdateStatistics, 921](#)
- [UpgradeContents, 923](#)
- [UpgradeExportedObjects, 925](#)

BackupContents

Sauvegarde le contenu du référentiel modèle dans un fichier. La commande échoue si le contenu du référentiel n'existe pas.

Pour garantir la création d'un fichier de sauvegarde cohérent, l'opération de sauvegarde bloque toutes les autres opérations du référentiel jusqu'à la fin de la sauvegarde.

La commande infacmd mrs BackupContents utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd mrs BackupContents :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de référentiel modèle.
OutputFileName -of	output_file_name	Obligatoire. Nom du fichier de sauvegarde.
OverwriteFile -ow	overwrite_file	Vous devez inclure cette option pour écraser un fichier de sauvegarde qui a le même nom.

Option	Argument	Description
Description -ds	description	Description du fichier de sauvegarde. Si la description contient des espaces ou d'autres caractères non alphabétiques, placez la description entre guillemets.
-BackupSearchIndices -bsi	-	Facultatif. Définissez comme « vrai » pour enregistrer l'index de recherche dans le fichier de sauvegarde et réduire le temps nécessaire pour restaurer le fichier. Réglez sur faux pour ne pas enregistrer l'index de recherche dans le fichier de sauvegarde. Lorsque vous restaurez le fichier, le service de référentiel modèle remet à jour l'index de recherche. La valeur par défaut est True.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

CheckInObject

Archive un seul objet extrait. L'objet est archivé dans le référentiel modèle.

La commande infacmd mrs CheckInObject utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd mrs CheckInObject :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-ObjectPathAndName -opn	MRS_object_path	Requis. Chemin de l'objet du référentiel modèle incluant le nom de l'objet. Placez le chemin entre guillemets doubles. Utilisez la syntaxe suivante : "ProjectName/FolderName/.../SubFolder_Name/{ObjectName ProjectName/ObjectName}"
-Description -ds	description	Facultatif. Vous pouvez utiliser ce paramètre pour la description de l'archivage ou des commentaires.

CreateContents

Crée le contenu de référentiel pour un référentiel modèle. La commande échoue si le contenu existe dans le référentiel modèle.

La commande infacmd mrs CreateContents utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd mrs CreateContents :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de référentiel modèle.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

CreateFolder

Crée un dossier dans un projet d'un référentiel modèle.

La syntaxe de la commande infacmd mrs CreateFolder est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments d'infacmd mrs CreateFolder :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-UserName -un	user_name	<p>Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>

Option	Argument	Description
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de référentiel modèle.
-ProjectName -pn	project_name	Obligatoire. Nom du projet dans lequel créer le dossier. Le nom du projet n'est pas sensible à la casse. Le nom du projet ne peut pas dépasser 128 caractères. Le nom du projet ne peut pas commencer par un nombre, et peut contenir des caractères alphanumériques et les caractères suivants : @ # _
-Path -p	folder_path_and_name	Obligatoire. Chemin et nom du dossier à créer. Le nom de chemin doit commencer par une barre oblique (/).
-CreatePath -cp	True False	Facultatif. Si la valeur est True, le dossier est créé dans le chemin spécifié. La valeur par défaut est False.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

CreateProject

Crée un projet dans un référentiel modèle.

La syntaxe de la commande infacmd mrs CreateProject est la suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd mrs CreateProject :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	Password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de référentiel modèle.

Option	Argument	Description
-ProjectName -pn	project_name	Obligatoire. Nom du projet à créer. Le nom du projet n'est pas sensible à la casse. Le nom du projet ne peut pas dépasser 128 caractères. Le nom du projet ne peut pas commencer par un nombre, et peut contenir des caractères alphanumériques et les caractères suivants : @ # _
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

CreateService

Crée un service de référentiel modèle. Avant de créer le service de référentiel modèle, vous devez créer une base de données pour stocker les tables du référentiel. Utilisez le client de base de données pour créer la base de données.

Chaque référentiel modèle doit répondre aux spécifications de la base de données suivantes :

- Le référentiel modèle doit avoir un schéma unique. Deux référentiels modèle ou le référentiel modèle et la base de données de configuration du domaine ne peuvent pas partager le même schéma.
- Le référentiel modèle doit avoir un nom de base de données du référentiel unique.

La commande infacmd mrs CreateService utilise la syntaxe suivante :

```
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,...]
```

Le tableau suivant décrit les options et arguments d'infacmd mrs CreateService :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
NodeName -nn	node_name	Requis. Nœud sur lequel vous souhaitez exécuter le service de référentiel modèle.
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-UserName -un	user_name	<p>Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>

Option	Argument	Description
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.
-DbUser -du	db_user	Requis. Compte de la base de données du référentiel. Configurez ce compte à l'aide du client de base de données.
-DbPassword -dp	db_password	Requis. Mot de passe de la base de données du référentiel pour l'utilisateur de la base de données.

Option	Argument	Description
-DbUrl -dl	db_url	<p>Requis.</p> <p>Chaîne de connexion JDBC permettant de se connecter à la base de données du référentiel modèle. Utilisez la syntaxe suivante pour chaque base de données prise en charge :</p> <ul style="list-style-type: none"> - IBM Db2. jdbc:informatica:db2://<host name>:<port number>;DatabaseName=<database name>;BatchPerformanceWorkaround=true;DynamicSections=3000 - Microsoft SQL Server qui utilise l'instance par défaut. jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true - Microsoft SQL Server qui utilise une instance nommée. jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true - Azure SQL Server. jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.<hostnamein certificate>;ValidateServerCertificate=true - Oracle. jdbc:informatica:oracle://<host name>:<port number>;SID=<database name>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true <p>Pour vous connecter à Oracle à l'aide du gestionnaire de connexions Oracle, utilisez la chaîne de connexion suivante :</p> <p>jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS server name>;</p> <ul style="list-style-type: none"> - PostgreSQL. jdbc:informatica:postgresql://<host name>:<port number>;DatabaseName=
-DbDriver -dr	db_driver	<p>Facultatif. Pilote Data Direct permettant de se connecter à la base de données. Par exemple :</p> <p>com.informatica.jdbc.oracle.OracleDriver</p>
-DbDialect -dd	db_dialect	<p>Facultatif. Dialecte SQL pour une base de données spécifiques. Le dialecte mappe des objets Java à des objets de base de données.</p> <p>Par exemple :</p> <p>org.hibernate.dialect.Oracle9Dialect</p>

Option	Argument	Description
-SearchIndexRoot -si	search_index_root	Facultatif. Change le répertoire de l'index de recherche. Entrez le chemin complet du répertoire. Le répertoire par défaut est le répertoire d'installation Informatica.
-DbType -dt	db_type	Facultatif. Les valeurs sont Oracle, SQL Server, DB2 ou PostgreSQL.
-DbSchema -ds	db_schema	Facultatif. Nom de schéma pour une base de données Microsoft SQL Server ou PostgreSQL.
-DbTablespace -dt	db_tablespace	Requis uniquement pour une base de données DB2. Lorsque vous configurez un nom d'espace de table, le service de référentiel modèle crée toutes les tables du référentiel dans le même espace de table. Le nom de l'espace de table ne doit pas contenir d'espaces.
[<-SecureJDBCParameters -sjdbc> secure_jdbc_parameters]	Paramètres JDBC sécurisés	Si la base de données du référentiel modèle est sécurisée via le protocole SSL, vous devez entrer les paramètres de base de données sécurisés. Entrez les paramètres sous la forme nom=valeur en les séparant par un point-virgule (;). Par exemple : param1=value1;param2=value2
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-FolderPath -fp	full_folder_path	Facultatif. Chemin d'accès complet, sans le nom de domaine, du dossier dans lequel vous souhaitez créer le service. Doit être au format suivant : <i>/parent_folder/child_folder</i> La valeur par défaut est « / » (le domaine).
-BackupNodes -bn	nodename1,nodename2,...	Facultatif. Nœuds sur lesquels le service peut s'exécuter si le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.

DeleteContents

Supprime le contenu du référentiel modèle. La commande échoue si le contenu n'existe pas dans le référentiel modèle.

La commande infacmd mrs DeleteContents utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd mrs DeleteContents :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-ServiceName -sn	service_name	Obligatoire. Nom du service de référentiel modèle.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

DeleteFolder

Supprime un dossier d'un projet dans un référentiel modèle.

Pour supprimer un dossier qui contient des objets, définissez l'option -ForceDelete sur True.

La commande infacmd mrs DeleteFolder utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd mrs DeleteFolder :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.
-ProjectName -pn	project_name	Requis. Nom du projet qui contient le dossier.
-Path -p	folder_path_and_name	Requis. Chemin et nom du dossier à supprimer. Le chemin doit commencer par une barre oblique (/).

Option	Argument	Description
-ForceDelete -f	True False	Facultatif. Si la valeur est True, cette option supprime un dossier qui contient des objets. La valeur par défaut est False.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

DeleteProject

Supprime un projet d'un référentiel modèle.

Pour supprimer un projet qui contient des dossiers et des objets, définissez l'option -ForceDelete sur True.

La commande infacmd mrs DeleteProject utilise la syntaxe suivante :

```
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]
```


Le tableau suivant décrit les options et les arguments de la commande infacmd mrs DeleteProject :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.
-ProjectName -pn	project_name	Requis. Nom du projet à supprimer.

Option	Argument	Description
-ForceDelete -f	True False	Facultatif. Si la valeur est True, cette option supprime un projet qui contient des dossiers et des objets. La valeur par défaut est False.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

disableMappingValidationEnvironment

Désactive l'environnement sélectionné de validation de mappages exécutés à partir de l'outil Developer tool.

Utilisez le paramètre ValidationEnvironment pour désactiver un environnement de validation pour un mappage. Répétez la commande pour chaque environnement à supprimer.

Utilisez les filtres pour mettre à jour un ou plusieurs mappages dans un projet. Si vous incluez des filtres, la commande met à jour tous les mappages non déployés vers le service d'intégration de données. Un mappage doit correspondre à tous les filtres spécifiés pour être modifié.

La commande infacmd mrs disableMappingValidationEnvironment utilise la syntaxe suivante :

```
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]
<-ValidationEnvironment|-ve> validation_environment_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

Le tableau suivant décrit les options et les arguments de la commande
disableMappingValidationEnvironment :

Option	Argument	Description
DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.
ProjectName -pn	project_name	Facultatif. Nom du projet qui contient le mappage. Si vous ne spécifiez pas de nom de projet, la commande met à jour tous les projets dans le référentiel modèle. Vous ne pouvez spécifier qu'un seul projet à la fois.

Option	Argument	Description
MappingNamesFilter -mnf	mapping_names	Facultatif. Noms des mappages pour lesquels vous voulez désactiver l'environnement de validation. Séparez les noms de mappage par des virgules. La valeur par défaut dans le référentiel modèle est Tous les mappages.
ExecutionEnvironmentFilter -eef	execution_environment_name	Facultatif. Spécifiez l'environnement d'exécution de l'environnement de validation à supprimer. Vous pouvez entrer Natif, Hadoop ou Databricks. Par défaut, l'environnement de validation est modifié pour tous les moteurs en fonction d'autres critères de filtre.
ValidationEnvironment -ve	validation_environment_name	Requis. Nom de l'environnement de validation à supprimer d'un mappage. Vous pouvez entrer l'une des valeurs suivantes : - natif - blaze - spark - spark-databricks Exécutez la commande pour chaque environnement de validation à supprimer.
ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

enableMappingValidationEnvironment

Active un environnement de validation pour les mappages exécutés à partir de l'outil Developer tool. Les propriétés d'environnement de validation de mappage indiquent les moteurs dans lesquels le mappage sera validé pour être exécuté.

Utilisez le paramètre ValidationEnvironment pour spécifier un environnement de validation à activer sur un mappage. Répétez la commande et spécifiez un environnement de validation différent pour activer un environnement de validation supplémentaire pour le mappage.

Utilisez les filtres pour mettre à jour un ou plusieurs mappages dans un projet. Si vous n'incluez pas de filtres, la commande met à jour tous les mappages non déployés vers le service d'intégration de données. Un mappage doit correspondre à tous les filtres spécifiés pour être modifié.

La commande infacmd mrs enableMappingValidationEnvironment utilise la syntaxe suivante :

```
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]
<-ValidationEnvironment|-ve> validation_environment_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]

```

Le tableau suivant décrit les options et les arguments de la commande
enableMappingValidationEnvironment :

Option	Argument	Description
DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.

Option	Argument	Description
ProjectName -pn	project_name	Facultatif. Nom du projet qui contient le mappage. Si vous ne spécifiez pas de nom de projet, la commande met à jour tous les projets dans le référentiel modèle. Vous ne pouvez spécifier qu'un seul projet à la fois.
ConnectionName -cn	connection_name	Nom de la connexion de l'environnement de validation de mappage à utiliser. La connexion remplace un paramètre de connexion existant ou un paramètre de connexion qui a été défini pour l'environnement. Requise pour activer l'environnement natif ou non natif si aucune connexion n'est présente dans le mappage spécifié. Facultatif pour activer l'environnement natif ou si une connexion est déjà présente.
MappingNamesFilter -mnf	mapping_names	Facultatif. Noms des mappages pour lesquels vous voulez activer l'environnement de validation. Séparez les noms de mappage par des virgules. La valeur par défaut dans le référentiel modèle est Tous les mappages.
ExecutionEnvironmentFilter -eef	execution_environment_name	Facultatif. Spécifiez l'environnement d'exécution sur lequel filtrer. Vous pouvez entrer Natif, Hadoop ou Databricks. Par défaut, l'environnement de validation est modifié pour tous les moteurs en fonction d'autres critères de filtre.
ValidationEnvironment -ve	validation_environment_name	Requis. Nom de l'environnement de validation à activer sur un mappage. Vous pouvez entrer l'une des valeurs suivantes : - natif - blaze - spark - spark-databricks Exécutez la commande pour chaque environnement de validation à activer.
ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

ListBackupFiles

Répertorie les fichiers du dossier de sauvegarde.

La commande infacmd mrs ListBackupFiles utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd ws ListBackupFiles :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-UserName -un	user_name	<p>Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>

Option	Argument	Description
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de référentiel modèle.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

ListCheckedOutObjects

Affiche une liste des objets extraits par un utilisateur. Exécutez cette commande sur un référentiel intégré à un système de contrôle de version.

La commande infacmd mrs listCheckedOutObjects utilise la syntaxe suivante :

```
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|-optype> operation_type]
```


Le tableau suivant décrit les options et les arguments de la commande `infacmd mrs listCheckedOutObjects` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-ByUser -bu	checkedout_by_user	Facultatif. Compte utilisateur dont le référentiel modèle contient des objets extraits.
-ObjectType -ot	object_type	Facultatif. Type de l'objet à rechercher. Par exemple, mappage.
-ByObjectPathandName -bopn	object_path_and_name	Facultatif. Chemin et nom de l'objet à rechercher.
-ObjectName -objn	object_name	Facultatif. Nom de l'objet à rechercher.
-LastOperationType -otype	operation_type	Facultatif. Type de l'opération à rechercher. Entrez l'une des valeurs suivantes : - ADD_OP - EDIT_OP - MOVE_OP - DELETE_OP

listFolders

Répertorie les noms de tous les dossiers contenus dans le chemin de dossier de projet spécifié.

L'option -Path vous permet de répertorier tous les dossiers d'un projet ou d'un sous-dossier. La barre oblique (/) vous permet de spécifier le niveau supérieur d'un projet.

Par exemple, la commande suivante répertorie tous les dossiers dans /MRS_1/Project_A/ :

```
infacmd mrs listFolders ... -sn MRS_1 -pn Project_A -p /
```

Si le contenu de Project_A est Folder_1 et Folder_2, la commande suivante répertorie tous les sous-dossiers de Folder_1 :

```
infacmd mrs listFolders ... -sn MRS_1 -pn Project_A -p /Folder_1/
```

La syntaxe de la commande infacmd mrs ListFolders est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments d'infacmd mrs ListFolders :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de référentiel modèle.

Option	Argument	Description
-ProjectName -pn	project_name	Obligatoire. Nom du projet pour lequel vous souhaitez répertorier les dossiers. Le nom du projet n'est pas sensible à la casse. Le nom du projet ne peut pas dépasser 128 caractères. Le nom du projet ne peut pas commencer par un nombre, et peut contenir des caractères alphanumériques et les caractères suivants : @ # _
-Path -p	path	Obligatoire. Chemin du dossier parent dans lequel vous voulez répertorier le contenu du dossier. Le chemin doit commencer par une barre oblique (/). Le nom n'est pas sensible à la casse.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

ListLockedObjects

Affiche une liste d'objets verrouillés par un utilisateur. Exécutez cette commande sur un référentiel non intégré à un système de contrôle de version.

Remarque: Si vous exécutez cette commande sur un référentiel avec version, la commande échoue.

La commande infacmd mrs listLockedObjects utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd mrs listLockedObjects` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-ByUser -bu	locked_by_user	Facultatif. Compte utilisateur qui possède le verrou sur les objets du référentiel modèle. Par défaut, les objets sont verrouillés par tous les utilisateurs.
-ObjectType -ot	object_type	Facultatif. Type de l'objet à rechercher. Vous pouvez exécuter la commande sur un type d'objet. Si vous omettez ce paramètre, la commande s'exécute sur tous les types d'objets.
-ByObjectPathAndName -bopn	object_path_and_name	Facultatif. Chemin et nom du référentiel modèle de l'objet à rechercher.
-ObjectName -objn	object_name	Facultatif. Nom de l'objet à rechercher.
-LastOperationType -otype	operation_type	Facultatif. Type de l'opération à rechercher. Entrez l'une des valeurs suivantes : - ADD_OP - EDIT_OP - MOVE_OP - DELETE_OP

listMappingEngines

Répertorie les moteurs d'exécution des mappages exécutés depuis l'outil Developer tool. Vous pouvez filtrer les résultats en fonction des paramètres du projet, de l'environnement de validation et de l'environnement d'exécution.

La syntaxe de la commande infacmd mrs listMappingEngines est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments d'infacmd mrs listMappingEngines :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.
ProjectName -pn	project_name	Facultatif. Nom du projet qui contient le mappage. Si vous ne spécifiez pas un nom de projet, la commande répertorie tous les projets et les mappages à l'intérieur de ceux-ci. Vous ne pouvez spécifier qu'un seul projet à la fois.

Option	Argument	Description
ValidationEnvironmentFilter -ve	validation_environment_name	Facultatif. Nom de l'environnement de validation pour lequel vous souhaitez afficher la liste des mappages. Choisissez l'une des valeurs suivantes : - natif - blaze - spark - spark-databricks Exécutez la commande de chaque environnement de validation pour répertorier les mappages.
ExecutionEnvironmentFilter -eef	execution_environment_name	Facultatif. Spécifiez l'environnement d'exécution selon lequel vous souhaitez filtrer les mappages. Choisissez Natif, Hadoop ou Databricks. Par exemple, lorsque vous spécifiez l'option Natif, la commande répertorie les mappages configurés pour s'exécuter sur le service d'intégration de données.
ExecutionEnvironmentParameterNameFilter -pnf	execution_environment_parameter_name	Facultatif. Spécifiez le nom du paramètre selon lequel vous pouvez paramétrer l'environnement d'exécution et le filtre. Vous pouvez paramétrer les environnements d'exécution dans le fichier de paramètres avec une variable et utiliser celle-ci dans la commande infacmd.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

listPermissionOnProject

Répertoriez toutes les autorisations dans plusieurs projets pour des groupes et utilisateurs. Séparez plusieurs noms de projets par une virgule. Il vous faut l'autorisation d'accès en lecture sur le projet pour afficher la liste des autorisations pour les groupes et utilisateurs.

La syntaxe de la commande infacmd mrs listPermissionOnProject est la suivante :

```
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]
```


Le tableau suivant décrit les options et les arguments d'infacmd mrs listPermissionOnProject :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	Password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de référentiel modèle.

Option	Argument	Description
-ProjectNames -pn	project_name_list	Obligatoire. Noms des projets pour lesquels vous souhaitez répertorier les autorisations pour les utilisateurs et groupes. Les noms de projets ne sont pas sensibles à la casse. Séparez plusieurs noms de projets par une virgule.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

ListProjects

Dresse la liste des projets dans le référentiel modèle. La commande échoue si le référentiel modèle n'a pas de contenu de référentiel.

La commande infacmd mrs ListProjects utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd mrs ListProjects :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de référentiel modèle.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

ListServiceOptions

Dresse la liste des options du service de référentiel modèle.

La commande infacmd mrs ListServiceOptions utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd mrs ListServiceOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-UserName -un	user_name	<p>Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>

Option	Argument	Description
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de référentiel modèle.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

ListServiceProcessOptions

Répertorie les options du processus de service de référentiel modèle.

La syntaxe de la commande infacmd mrs ListServiceProcessOptions est la suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd mrs ListServiceProcessOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
NodeName -nn	node_name	Obligatoire. Nom de nœud pour lequel vous souhaitez répertorier les options du processus de service.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-UserName -un	user_name	<p>Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>
-Password -pd	password	<p>Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p>
-ServiceName -sn	service_name	Obligatoire. Nom du service de référentiel modèle.
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>

ManageGroupPermissionOnProject

Gère les autorisations sur plusieurs projets pour un groupe.

La commande infacmd mrs manageGroupPermissionOnProject utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd mrs manageGroupPermissionOnProject :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-recipientSecurityDomain -rdn	recipient_security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel le groupe de destinataires est rattaché. Pour définir le domaine de sécurité du destinataire, reportez-vous aux mêmes instructions que celles que vous utilisez pour définir le domaine de sécurité de l'utilisateur d'autorisation.

Option	Argument	Description
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.
-ProjectNames -pn	project_name_list	Requis. Noms des projets pour lesquels vous souhaitez autoriser ou révoquer des autorisations. Les noms de projets ne sont pas sensibles à la casse. Séparez plusieurs noms de projets par une virgule.
-Permission -pm	permission_name	Requis. Autorisations que vous souhaitez autoriser ou révoquer du groupe de destinataires. Entrez l'autorisation entre guillemets doubles et utilisez une barre oblique inverse (\) comme caractère d'échappement. Les arguments suivants sont valides : +r, +w, +g, -r, -w, -g Utilisez ces arguments pour autoriser ou révoquer les autorisations de lecture, d'écriture et d'octroi. Par exemple, un argument valide pour révoquer les autorisations de lecture et autoriser les autorisations d'écriture est \ "-r+w\".
-RecipientName -rn	recipient_name	Requis. Nom du groupe de destinataires pour lequel vous souhaitez gérer les autorisations.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

ManageUserPermissionOnProject

Gère les autorisations sur plusieurs projets pour un utilisateur.

La commande `infacmd mrs manageUserPermissionOnProject` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande `infacmd mrs manageUserPermissionOnProject` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-recipientSecurityDomain -rdn	recipient_security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel le destinataire est rattaché. Pour définir le domaine de sécurité du destinataire, reportez-vous aux mêmes instructions que celles que vous utilisez pour définir le domaine de sécurité de l'utilisateur d'autorisation.

Option	Argument	Description
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.
-ProjectNames -pn	project_name_list	Requis. Noms des projets pour lesquels vous souhaitez autoriser ou révoquer des autorisations. Les noms de projets ne sont pas sensibles à la casse. Séparez plusieurs noms de projets par une virgule.
-Permission -pm	permission_name	Requis. Autorisations que vous souhaitez autoriser ou révoquer du groupe de destinataires. Entrez l'autorisation entre guillemets doubles et utilisez une barre oblique inverse (\) comme caractère d'échappement. Les arguments suivants sont valides : +r, +w, +g, -r, -w, -g Utilisez ces arguments pour autoriser ou révoquer les autorisations de lecture, d'écriture et d'octroi. Par exemple, un argument valide pour révoquer les autorisations de lecture et autoriser les autorisations d'écriture est \ "-r+w\".
-RecipientName -rn	recipient_name	Requis. Nom d'utilisateur du destinataire pour lequel vous souhaitez gérer les autorisations.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

PopulateVCS

Synchronise le référentiel modèle avec un système de contrôle de version. Pour pouvoir synchroniser le référentiel modèle avec un système de contrôle de version, vous devez préalablement configurer les propriétés de contrôle de version.

Lorsque vous configurez les propriétés de contrôle de version, vous redémarrez le référentiel modèle et vous exécutez la commande PopulateVCS.

Remarque: Après avoir exécuté la commande, le référentiel modèle est indisponible jusqu'à la fin de la synchronisation.

La commande infacmd mrs populateVCS utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd mrs populateVCS :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>

Option	Argument	Description
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

ReassignCheckedOutObject

Réattribue la propriété d'un objet extrait à un autre utilisateur. Si le propriétaire d'un objet extrait a enregistré des modifications, celles-ci sont conservées lorsque vous réattribuez l'objet. Si les modifications ne sont pas enregistrées, elles sont perdues.

La commande infacmd mrs reassignCheckedOutObject utilise la syntaxe suivante :

```
<-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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd mrs reassignCheckedOutObject` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-ObjectPathAndName -opn	MRS_object_path	Requis. Utilisez la syntaxe suivante : ProjectName/FolderName/.../SubFolder_Name/ {ObjectName ProjectName/ObjectName}
-ToUser -tu	Username	Requis. Nom de l'utilisateur auquel vous voulez attribuer l'état d'objet extrait.
-ToUserSecurityDomain -tsd	Security domain	Facultatif. Domaine de sécurité de l'utilisateur auquel vous voulez attribuer l'état d'objet extrait.

rebuildDependencyGraph

Reconstruit le graphique de dépendance d'objet pour que vous puissiez afficher les dépendances d'objets après la mise à niveau. Exécutez cette commande si la mise à niveau du service de référentiel modèle ne peut pas reconstruire le graphique de dépendance d'objet.

Les utilisateurs ne doivent pas accéder aux objets du référentiel modèle tant que le processus de régénération n'est pas terminé, car cela risque de rendre le graphique de dépendance d'objet inexact. Vous pouvez exécuter la commande lorsque les utilisateurs ne sont pas connectés.

La commande `infacmd mrs rebuildDependencyGraph` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd mrs rebuildDependencyGraph` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de référentiel modèle.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

RenameFolder

Renomme un dossier dans un projet.

La syntaxe de la commande infacmd mrs RenameFolder est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments d'infacmd mrs RenameFolder :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-UserName -un	user_name	<p>Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>

Option	Argument	Description
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de référentiel modèle.
-ProjectName -pn	project_name	Obligatoire. Nom du projet qui contient le dossier à renommer.
-SourceFolder -sf	source_folder_path_and_name	Obligatoire. Chemin et nom du dossier à renommer. Le chemin doit commencer par une barre oblique (/).
-TargetFolder -tn	target_folder_path_and_name	Obligatoire. Nouveau nom du dossier. Vous pouvez spécifier un nom de dossier ou un chemin et un nom de dossier. Le chemin doit commencer par une barre oblique (/).
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

replaceMappingHadoopRuntimeConnections

Remplace la connexion Hadoop de tous les mappages dans le référentiel par une autre connexion Hadoop. Le Service d'intégration de données utilise la connexion Hadoop pour se connecter au cluster Hadoop pour exécuter des mappages dans l'environnement Hadoop.

La commande ne modifie pas les connexions Hadoop dans les transformations. Vous pouvez spécifier le nom du projet pour remplacer la connexion Hadoop des mappages dans le projet.

La commande infacmd mrs replaceMappingHadoopRuntimeConnections utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `replaceMappingHadoopRuntimeConnections` :

Option	Argument	Description
DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
ServiceName -sn	service_name	Requis. Nom du service d'intégration de données.
ProjectName -an	application_name	Facultatif. Nom du projet qui contient le mappage. Si vous spécifiez cette option, la commande remplace la connexion Hadoop uniquement pour le projet.
OldConnectionName -oc	connection_name_of_old_connection_to_replace	Requis. Nom de la connexion Hadoop à remplacer.
NewConnectionName -nc	connection_name_of_new_connection	Requis. Nom de la connexion Hadoop que le service d'intégration de données doit utiliser pour se connecter à la grappe Hadoop afin d'exécuter des mappages dans l'environnement Hadoop.
ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

RestoreContents

Restaure le contenu d'un référentiel modèle depuis un fichier de sauvegarde.

La commande infacmd mrs RestoreContents utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et arguments d'infacmd mrs RestoreContents :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de référentiel modèle à sauvegarder.

Option	Argument	Description
InputFileName -if	input_file_name	Obligatoire. Nom du fichier de sauvegarde à restaurer.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

UndoCheckout

Rétablit l'extraction d'un objet du référentiel modèle. L'objet est archivé dans le référentiel modèle. Le référentiel modèle ignore les modifications apportées à l'objet, car il a été extrait. Le système de contrôle de version n'incrmente pas le numéro de version ou ne l'ajoute pas à l'historique des versions.

La commande infacmd mrs undoCheckout utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd mrs undoCheckout` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ObjectPathAndName -opn	MRS_object_path	Requis. Chemin de l'objet du référentiel modèle incluant le nom de l'objet. Placez le chemin entre guillemets doubles. Utilisez la syntaxe suivante : "ProjectName/FolderName/.../SubFolder_Name/{ObjectName ProjectName/ObjectName}"

setMappingExecutionEnvironment

Spécifie l'environnement d'exécution des mappages exécutés à partir de l'outil Developer tool.

Utilisez les filtres pour mettre à jour un ou plusieurs mappages dans un projet. Si vous n'incluez pas de filtres, la commande met à jour tous les mappages non déployés vers le service d'intégration de données. Un mappage doit correspondre à tous les filtres spécifiés pour être modifié.

La commande infacmd mrs setMappingExecutionEnvironment utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `setMappingExecutionEnvironment` :

Option	Argument	Description
DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.
ProjectName -pn	project_name	Facultatif. Nom du projet qui contient le mappage. Si vous ne spécifiez pas de nom de projet, la commande met à jour tous les projets dans le référentiel modèle.
MappingNamesFilter -mnf	mapping_names	Facultatif. Noms des mappages pour lesquels vous souhaitez définir l'environnement d'exécution. Séparez les noms de mappage par des virgules. La valeur par défaut est tous les mappages non déployés.

Option	Argument	Description
ExecutionEnvironment -ee	execution_environment_name	Requis. Nom de l'environnement d'exécution à définir. Choisissez Natif, Hadoop ou Databricks.
ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

UndoCheckout

Rétablit l'extraction d'un objet du référentiel modèle. L'objet est archivé dans le référentiel modèle. Le référentiel modèle ignore les modifications apportées à l'objet, car il a été extrait. Le système de contrôle de version n'incrmente pas le numéro de version ou ne l'ajoute pas à l'historique des versions.

La commande infacmd mrs undoCheckout utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd mrs undoCheckout` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ObjectPathAndName -opn	MRS_object_path	Requis. Chemin de l'objet du référentiel modèle incluant le nom de l'objet. Placez le chemin entre guillemets doubles. Utilisez la syntaxe suivante : "ProjectName/FolderName/.../SubFolder_Name/{ObjectName ProjectName/ObjectName}"

UnlockObject

Déverrouille un objet du référentiel modèle verrouillé par un utilisateur. Exécutez cette commande sur un référentiel non intégré à un système de contrôle de version.

Remarque: Si vous exécutez cette commande sur un référentiel avec version, la commande échoue.

Vous pouvez déverrouiller un seul objet à la fois.

La commande infacmd mrs unlockObject utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd mrs unlockObject` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ObjectPathAndName -opn	MRS_object_path	Requis. Chemin de l'objet du référentiel modèle incluant le nom de l'objet. Par exemple, utilisez la syntaxe suivante : ProjectName/FolderName/SubFolder_Name/ObjectName

UpdateServiceOptions

Met à jour les options du service de référentiel modèle. Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

La commande infacmd mrs UpdateServiceOptions utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd mrs UpdateServiceOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-Options -o	options	Requis. Entrez la paire nom-valeur séparée par des espaces.
-PrimaryNode -nn	primary node name	Facultatif. Nœud sur lequel vous souhaitez exécuter le service de référentiel modèle.
-BackupNodes -bn	nodename1,nodename2,...	Facultatif. Nœuds sur lesquels le service peut s'exécuter si le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.
-SearchIndexRoot -si		Facultatif. Change le répertoire de l'index de recherche. Entrez le chemin complet du répertoire. Le répertoire par défaut est le répertoire d'installation Informatica.

Options du service de référentiel modèle

Utilisez les options du service de référentiel modèle avec la commande `infacmd mrs UpdateServiceOptions`.

Entrez les options du service de référentiel modèle au format suivant :

```
... -o option_name=value option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options du service de référentiel modèle :

Option	Argument	Description
CACHE.EnableCache	True False	Permet au service de référentiel modèle de stocker des objets du référentiel modèle dans la mémoire cache. Pour appliquer les modifications, redémarrez le service de référentiel modèle.
CACHE.CacheJVMOptions	-Xmx[heap_size]	Options JVM du cache du service de référentiel modèle. Pour configurer la quantité de mémoire allouée au cache, configurez la taille maximale du tas mémoire. Ce champ doit inclure la taille maximale du tas mémoire spécifiée par l'option -Xmx. La valeur par défaut et la valeur minimale de la taille maximale du tas mémoire sont -Xmx128m. Les options que vous configurez s'appliquent lorsque le cache du service de référentiel modèle est activé. Pour appliquer les modifications, redémarrez le service de référentiel modèle. Les options que vous configurez dans ce champ ne s'appliquent pas à la machine virtuelle Java (JVM) qui exécute le service de référentiel modèle.
PERSISTENCE_DB.Username	db_user	Obligatoire. Compte de la base de données du référentiel. Configurez ce compte à l'aide du client de base de données.

Option	Argument	Description
PERSISTENCE_DB.Password	db_password	Obligatoire. Mot de passe de la base de données du référentiel pour l'utilisateur de la base de données.
PERSISTENCE_DB.DatabaseSchema	db_schema	Facultatif. Nom du schéma d'une base de données spécifique.
PERSISTENCE_DB.DatabaseTablespace	db_tablespace	Obligatoire uniquement pour une base de données DB2. Lorsque vous configurez un nom d'espace de table, le service de référentiel modèle crée toutes les tables du référentiel dans le même espace de table. Le nom de l'espace de table ne doit pas contenir d'espaces. Pour une base de données IBM DB2 à partitions multiples, l'espace de table doit s'étendre sur un seul nœud et une seule partition.
PERSISTENCE_DB.DatabaseType	DatabaseType	Obligatoire. Les types de base de données sont les suivants : <ul style="list-style-type: none"> - db2 - oracle - mssqlserver - sybase

Option	Argument	Description
PERSISTENCE_DB.JDBCConnectString	Chaîne de connexion JDBC	<p>Chaîne de connexion JDBC permettant de se connecter à la base de données du référentiel modèle. Utilisez la syntaxe suivante pour chaque base de données prise en charge :</p> <ul style="list-style-type: none"> - IBM Db2. jdbc:informatica:db2://<host name>:<port number>;DatabaseName=<database name>;BatchPerformanceWorkaround=true;DynamicSections=3000 - Microsoft SQL Server qui utilise l'instance par défaut. jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true - Microsoft SQL Server qui utilise une instance nommée. jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true - Azure SQL Server. jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.<hostname incertificate>;ValidateServerCertificate=true - Oracle. jdbc:informatica:oracle://<host name>:<port number>;SID=<database name>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true <p>Pour vous connecter à Oracle à l'aide du gestionnaire de connexions Oracle, utilisez la chaîne de connexion suivante :</p> <p>jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS server name>;</p> - PostgreSQL. jdbc:informatica:postgres://<host name>:<port number>;DatabaseName=
PERSISTENCE_DB.SecureJDBCParameters	Paramètres JDBC sécurisés	<p>Si la base de données du référentiel modèle est sécurisée via le protocole SSL, vous devez entrer les paramètres de base de données sécurisés.</p> <p>Entrez les paramètres sous la forme nom=valeur en les séparant par un point-virgule (;). Par exemple :</p> <p>param1=value1;param2=value2</p>
PERSISTENCE_DB.Dialect	Dialect	<p>Dialecte SQL pour une base de données spécifiques. Le dialecte mappe des objets Java à des objets de base de données.</p> <p>Par exemple :</p> <p>org.hibernate.dialect.Oracle9Dialect</p>

Option	Argument	Description
PERSISTENCE_DB.Driver	Driver	Pilote Data Direct permettant de se connecter à la base de données. Par exemple : <code>com.informatica.jdbc.oracle.OracleDriver</code>
SEARCH.SearchAnalyzer	Nom de classe Java complet	Nom de classe Java complet de l'analyseur de recherche. Par défaut, le service de référentiel modèle utilise l'analyseur de recherche suivant pour l'anglais : <code>com.informatica.repository.service.provider.search.analysis.MMStandardAnalyzer</code> Vous pouvez indiquer le nom de classe Java suivant pour l'analyseur de recherche en chinois, japonais et coréen : <code>org.apache.lucene.analysis.cjk.CJKAnalyzer</code> Vous pouvez également créer et spécifier un analyseur de recherche personnalisé.
SEARCH.SearchAnalyzerFactory	Nom de classe Java complet	Nom de classe Java complet de la classe de fabrique si vous avez utilisé une classe de fabrique lors de la création d'un analyseur de recherche personnalisé. Si vous utilisez un analyseur de recherche personnalisé, entrez le nom de la classe de l'analyseur de recherche ou de la classe de fabrique de l'analyseur de recherche.
VCS.Host	IP_address or host name	Obligatoire pour configurer les propriétés de contrôle de version pour le référentiel modèle sur Perforce. URL, adresse IP ou nom d'hôte de la machine sur laquelle le système de contrôle de version Perforce s'exécute. N'utilisez pas cette option lorsque vous configurez SVN ou Git comme système de contrôle de version.
VCS.URL	URL du référentiel de sous-version	Obligatoire pour configurer les propriétés de contrôle de version pour le référentiel modèle sur SVN et Git. URL du référentiel de sous-version. Par exemple : <code>VCS.URL=https://myserver.company.com/svn/</code> N'utilisez pas cette option lorsque vous configurez Perforce comme système de contrôle de version.
VCS.Port	VCS_port	Obligatoire pour configurer les propriétés de contrôle de version pour le référentiel modèle. Numéro de port que l'hôte du système de contrôle de version utilise pour écouter les paquets du référentiel modèle.

Option	Argument	Description
VCS.User	VCS_user	<p>Obligatoire pour configurer les propriétés de contrôle de version pour le référentiel modèle.</p> <p>Compte utilisateur de l'utilisateur du système de contrôle de version.</p> <p>Ce compte doit disposer d'autorisations d'accès en écriture sur le système de contrôle de version. Après avoir configuré la connexion avec l'utilisateur et le mot de passe du système de contrôle de version, tous les utilisateurs du référentiel modèle se connectent au système de contrôle de version via ce compte.</p> <p>Pour le système de contrôle de version Perforce, le type de compte doit correspondre à un utilisateur standard.</p>
VCS.Password	VCS_password	<p>Obligatoire pour configurer les propriétés de contrôle de version pour le référentiel modèle.</p> <p>Mot de passe de l'utilisateur du système de contrôle de version.</p>
VCS.Type	VCS_type	<p>Obligatoire pour configurer les propriétés de contrôle de version pour le référentiel modèle.</p> <p>Système de contrôle de version pris en charge auquel vous souhaitez vous connecter. Vous pouvez choisir Perforce, SVN ou Git.</p>
VCS.MRSPath	MRS_path	<p>Obligatoire pour configurer les propriétés de contrôle de version pour le référentiel modèle sur Perforce.</p> <p>Chemin du répertoire racine de la copie des objets du référentiel modèle du système de contrôle de version.</p> <p>Remarque: Lorsque vous exécutez la commande, le référentiel modèle se connecte au système de contrôle de version et génère le répertoire spécifié s'il n'existe pas encore.</p> <p>Un seul service de référentiel modèle peut utiliser ce répertoire.</p> <p>Pour Perforce, utilisez la syntaxe suivante :</p> <pre>//directory/path</pre> <p>Où <code>directory</code> est la racine du répertoire Perforce et <code>path</code> la suite du chemin du répertoire racine des objets du référentiel modèle.</p> <p>Exemple :</p> <pre>//depot/Informatica/repository_copy</pre> <p>N'utilisez pas cette option lorsque vous configurez SVN ou Git comme système de contrôle de version.</p>

UpdateServiceProcessOptions

Met à jour les options du processus de service pour le Service de Référentiel Modèle. Séparez les options multiples par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Entrez les options de processus de service au format suivant :

```
... -o "option_name=value option_name=value" ...
```

Place tous les noms et valeurs d'option entre guillemets doubles.

La syntaxe de la commande infacmd mrs UpdateServiceProcessOptions est la suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd mrs UpdateServiceProcessOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
NodeName -nn	node_name	Requis. Nom de nœud pour lequel vous voulez définir les options de processus.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de référentiel modèle.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Options -o	options	Requis. Entrez la paire nom-valeur séparée par des espaces. Entrez les options en utilisant le format suivant : OptionGroupName.OptionName=OptionValue OptionGroupName2.OptionName2=OptionValue2

UpdateStatistics

Mettez à jour les statistiques du référentiel de modèle sur Microsoft SQL Server. Vous pouvez exécuter cette commande si vous disposez du privilège d'administrateur système pour la base de données Microsoft SQL Server.

La syntaxe de la commande infacmd mrs updateStatistics est la suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd mrs updateStatistics :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-ServiceName -sn	service_name	Obligatoire. Nom du service de référentiel modèle.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

UpgradeContents

Met à niveau le contenu du référentiel modèle. La commande échoue si le référentiel modèle n'a pas de contenu de référentiel.

La commande infacmd mrs UpgradeContents utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd mrs UpgradeContents :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de référentiel modèle.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

UpgradeExportedObjects

Met à niveau les objets exportés vers un fichier .xml à partir d'une version précédente d'Informatica vers le format de métadonnées actuel. La commande génère ensuite un fichier .xml contenant les objets mis à niveau.

La commande met à niveau les objets exportés à partir d'un référentiel modèle Informatica 10.1 ou ultérieur. Importez le fichier .xml contenant les objets mis à niveau dans un référentiel modèle de version actuelle.

Le processus de mise à niveau dépend du service de référentiel modèle. Vous devez indiquer le nom de service d'un service de référentiel modèle exécuté dans le domaine lorsque vous exécutez la commande.

La commande infacmd mrs UpgradeExportedObjects utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd mrs UpgradeExportedObjects :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>

Option	Argument	Description
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom d'un service de référentiel modèle Informatica 10.2 s'exécutant dans le domaine.
-SourceFile -sf	source_file	Requis. Chemin d'accès et nom du fichier .xml qui contient les objets à mettre à niveau. Vous pouvez spécifier un chemin absolu ou relatif pour le fichier.
-TargetFile -tf	target_file	Requis. Chemin d'accès et nom du fichier .xml généré contenant les objets mis à niveau. Vous pouvez spécifier un chemin absolu ou relatif pour le fichier.
OverwriteFile -ow	overwrite_file	Facultatif. Vous devez inclure cette option pour remplacer le fichier cible qui a le même nom.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

CHAPITRE 26

Référence de commande d'infacmd ms

Ce chapitre comprend les rubriques suivantes :

- [abortAllJobs, 927](#)
- [deleteMappingPersistedOutputs, 929](#)
- [fetchAggregatedClusterLogs, 931](#)
- [getMappingStatus, 933](#)
- [getRequestLog, 935](#)
- [ListMappingOptions, 937](#)
- [listMappingParams, 939](#)
- [listMappingPersistedOutputs, 941](#)
- [listMappings, 943](#)
- [purgeDatabaseWorkTables, 945](#)
- [runMapping, 947](#)
- [UpdateMappingOptions, 952](#)
- [UpdateOptimizationDefaultLevel, 954](#)
- [UpdateOptimizationLevel, 956](#)
- [upgradeMappingParameterFile, 958](#)

abortAllJobs

Abandonne toutes les tâches de mappage déployées dans le service d'intégration de données.

Cette commande concerne les tâches déployées qui sont configurées pour être exécutées sur le moteur Spark. Elle concerne également les tâches de la file d'attente stockées dans le référentiel modèle configuré dans les propriétés du service d'intégration de données. Cette commande abandonne les tâches de lots que vous exécutez depuis infacmd.

Pour les tâches à la demande, la commande abandonne les tâches sur l'un des nœuds du service d'intégration de données et n'affecte pas d'autres nœuds du domaine.

Remarque: Il n'est pas possible de spécifier le nœud sur lequel la commande abandonne les tâches à la demande.

Vous pouvez utiliser des indicateurs facultatifs pour appliquer la commande uniquement à des tâches en files d'attente ou en cours d'exécution. Si vous n'incluez aucune des deux options, cette commande concerne toutes les tâches.

Cette commande échoue si vous l'exécutez lors des opérations de nettoyage Spark.

La commande `infacmd ms abortAllJobs` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd ms abortAllJobs` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-OnlyQueuedJobs -q	true false	Facultatif. Cette option permet de filtrer les tâches concernées afin de n'inclure que celles que le service d'intégration de données a mises en file d'attente pour l'exécution.
-OnlyRunningJobs -r	true false	Facultatif. Cette option permet de filtrer les tâches concernées afin de n'inclure que celles que le service d'intégration de données est en train d'exécuter.

deleteMappingPersistedOutputs

Supprime toutes les sorties de mappage persistantes d'un mappage déployé. Spécifiez les sorties à supprimer à l'aide du nom de l'application et du nom d'instance d'exécution du mappage. Pour utiliser des sorties spécifiques, utilisez l'option -OutputNamesToDelete.

La commande infacmd ms deleteMappingPersistedOutputs utilise la syntaxe suivante :

```
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]

```

Le tableau suivant décrit les options et les arguments de la commande `infacmd ms deleteMappingPersistedOutputs` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui a exécuté le mappage.
-Application -a	application_name	Requis. Nom de l'application qui contient le mappage.
-RuntimeInstanceName -rin	runtime_instance_name	Obligatoire. Nom de l'instance d'exécution du mappage. Utilisez le nom spécifié dans la commande infacmd ms runMapping pour exécuter les commandes listMappingPersistedOutputs et deleteMappingPersistedOutputs.
-OutputNamesToDelete -ontd	output_names_to_delete	Facultatif. Noms des sorties persistantes à supprimer. Pour spécifier plusieurs sorties pour suppression, séparez les noms par une virgule.

fetchAggregatedClusterLogs

Obtient le fichier .zip ou .tar.gz des journaux de cluster agrégés pour un mappage basé sur l'ID de la tâche et enregistre le fichier journal agrégé compressé dans un répertoire cible.

La commande infacmd ms fetchAggregatedClusterLogs utilise la syntaxe suivante :

```

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]

```

Le tableau suivant décrit les options et les arguments de la commande `infacmd ms fetchAggregatedClusterLogs` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui a exécuté le mappage.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-RequestId -id	request_id	Obligatoire. ID de tâche du mappage pour lequel vous souhaitez écrire le fichier journal. Entrez l'ID de tâche renvoyé par la commande <code>infacmd ms runMapping</code> .
-TargetLogDirectory -tld	target_log_directory	Facultatif. Répertoire dans lequel vous souhaitez enregistrer le fichier journal agrégé compressé.
-TargetFilename -tf	nom de fichier cible sans extension	Facultatif. Nom et chemin d'accès du fichier journal agrégé compressé.
-ClusterLoginUsername -clu	cluster_login_username	Requis si vous utilisez une application ResourceManager YARN compatible Kerberos. Nom d'utilisateur pour accéder à l'application YARN.
-ClusterLoginPassword -clp	cluster_login_password	Requis si vous spécifiez le nom d'utilisateur de connexion du cluster. Mot de passe pour accéder à l'application YARN. Le mot de passe est sensible à la casse.
-CustomProperties -cp	custom_properties	Facultatif. Définissez les propriétés personnalisées d'un mappage à la demande du support client international Informatica. Entrez les propriétés personnalisées en tant que paires nom-valeur séparées par des points-virgules. Par exemple : ... -cp custom_property_name=value Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

getMappingStatus

Obtient le statut actuel d'une tâche de mappage déployée par ID de tâche. Entrez l'ID de tâche renvoyé par la commande `infacmd ms runMapping`.

Remarque: Vous devez configurer le service de référentiel modèle de surveillance dans l'outil Administrator tool avant d'utiliser cette commande.

La syntaxe de la commande `infacmd ms getMappingStatus` est la suivante :

```
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]
```

La commande renvoie des informations sur l'exécution d'un mappage, y compris le nom de la tâche, l'état de la tâche et le chemin du fichier journal.

Si un nom d'instance d'exécution est transmis avec la commande runMapping, le nom de la tâche est le nom de l'instance d'exécution. Dans le cas contraire, le nom de la tâche est l'une des options suivantes :

- <mapping name>
- <mapping name>_<parameter set name>
- <mapping name>_<parameter file name>

Le tableau suivant décrit les options et les arguments de la commande infacmd ms getMappingStatus :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui a exécuté le mappage.
-JobId -jl	job_id	Requis. ID de la tâche de mappage dont vous souhaitez obtenir le statut. Entrez l'ID de tâche renvoyé par la commande infacmd ms runMapping.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

getRequestLog

Écrit le journal de mappage dans le fichier spécifié. Entrez l'ID de tâche renvoyé par la commande infacmd ms runMapping.

La syntaxe de la commande infacmd ms getRequestLog est la suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande infacmd ms getRequestLog :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui a exécuté le mappage.

Option	Argument	Description
-UserName -un	user_name	<p>Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>
-Password -pd	mot de passe	<p>Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p> <p>Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.</p>
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p> <p>Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>

Option	Argument	Description
-RequestId -id	request_id	Requis. ID de tâche du mappage pour lequel vous souhaitez écrire le fichier journal. Entrez l'ID de tâche renvoyé par la commande infacmd ms runMapping.
-FileName -f	file_name	Requis. Nom et chemin de l'emplacement dans lequel vous souhaitez écrire le fichier journal.

ListMappingOptions

Répertorie les options de mappage dans une application.

La syntaxe de la commande infacmd ms listMappingOptions est la suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande infacmd ms listMappingOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire. Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation. Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec ces deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui exécute le mappage. L'application qui contient le mappage doit être déployée dans un service d'intégration de données.
-Application -a	application_name	Requis. Nom de l'application qui contient le mappage.
-Mapping -m	mapping_name	Requis. Nom du mappage.

listMappingParams

Répertorie les paramètres d'un mappage et crée un fichier de paramètres de mappage que vous pouvez utiliser lorsque vous exécutez un mappage. La commande renvoie un fichier XML avec des valeurs par défaut que vous pouvez mettre à jour. Entrez le nom du fichier de paramètres lorsque vous exécutez le mappage avec la commande `infacmd ms runMapping`.

La syntaxe de la commande `infacmd ms listMappingParams` est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd ms listMappingParams` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui exécute le mappage. L'application qui contient le mappage doit être déployée dans un service d'intégration de données.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire. Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation. Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application_name	Requis. Nom de l'application qui contient le mappage.
-Mapping -m	mapping_name	Requis. Nom du mappage.
- OutputFile - o	sortie file_to_write_to	Facultatif. Chemin et nom du fichier de paramètres à créer. Si vous ne spécifiez pas de fichier, la commande affiche les paramètres dans l'invite de commande.

Sortie de listMappingParams

La commande `listMappingParams` renvoie un fichier de paramètres sous la forme d'un fichier XML avec des valeurs par défaut que vous pouvez mettre à jour.

Par exemple, vous exécutez la commande `listMappingParams` dans l'application « MyApp » et le mappage « MyMapping ». Le mappage « MyMapping » dispose d'un paramètre « MyParameter. » La commande `listMappingParams` renvoie un fichier XML au format suivant :

```
<?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>
```

Le fichier XML de sortie contient les éléments de niveau supérieur suivants :

Élément d'application

Lorsque vous définissez un paramètre dans l'élément de niveau supérieur de l'application, le service d'intégration de données applique la valeur du paramètre lorsque vous exécutez le mappage spécifique dans l'application spécifique. Vous devez inclure au moins un élément de projet dans un élément d'application/mappage.

Par défaut, cet élément de niveau supérieur se trouve entre commentaires. Retirez les commentaires (! -- et -- >) pour utiliser cet élément.

Élément de projet

Lorsque vous définissez un paramètre dans un élément de niveau supérieur du projet, le service d'intégration de données applique la valeur du paramètre au mappage spécifique dans le projet dans toute application déployée. Le service applique également la valeur du paramètre à tout mappage qui utilise les objets dans le projet.

Si vous définissez le même paramètre dans un élément de projet ou d'application de niveau supérieur dans le même fichier de paramètres, la valeur des paramètres définie dans l'élément d'application est prioritaire.

listMappingPersistedOutputs

Répertorie les sorties de mappage persistantes pour un mappage déployé. Les sorties sont répertoriées selon le nom de l'application et le nom d'instance d'exécution du mappage.

La commande `infacmd ms listMappingPersistedOutputs` utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et les arguments de la commande `infacmd ms listMappingPersistedOutputs` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui a exécuté le mappage.
-Application -a	application_name	Requis. Nom de l'application qui contient le mappage.
-RuntimeInstanceName -rin	runtime_instance_name	Obligatoire. Nom de l'instance d'exécution du mappage. Utilisez le nom spécifié dans la commande infacmd ms runMapping pour exécuter les commandes listMappingPersistedOutputs et deleteMappingPersistedOutputs.

listMappings

Répertorie les mappages dans une application.

La syntaxe de la commande infacmd ms listMappings est la suivante :

```
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

Le tableau suivant décrit les options et les arguments de la commande `infacmd ms listMappings` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire. Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation. Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec ces deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui exécute le mappage. L'application qui contient le mappage doit être déployée dans un service d'intégration de données.
-Application -a	application_name	Requis. Nom de l'application qui contient le mappage.

purgeDatabaseWorkTables

Purge les informations de toutes les tâches de la file d'attente lorsque vous activez la récupération Data Engineering pour le service d'intégration de données.

Cette commande purge les files d'attente de travail, certaines informations sur les tâches en cours d'exécution, ainsi que les informations de récupération Data Engineering. Elle supprime les lignes des tables de base de données des tâches en file d'attente et en cours d'exécution. Utilisez cette commande pour supprimer les informations des tâches restantes dans la base de données du référentiel modèle après avoir supprimé le service d'intégration de données configuré pour la récupération Data Engineering.

Cette commande concerne les tâches du référentiel modèle configuré dans les propriétés du service d'intégration de données. Vous pouvez utiliser l'option -msn pour spécifier un référentiel modèle différent.

Vous pouvez utiliser l'option -q pour appliquer la commande uniquement à des tâches en file d'attente.

Vous pouvez exécuter la commande uniquement à l'arrêt du service d'intégration de données.

La commande infacmd ms purgeDatabaseWorkTables utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd ms purgeDatabaseWorkTables` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-OnlyQueuedJobs -q	true false	Facultatif. Cette option permet de filtrer les résultats afin de n'inclure que les tâches que le service d'intégration de données a mises en file d'attente pour l'exécution.
-MrsName -msn	Model_repository_service_name	Facultatif. Nom du service de référentiel modèle à partir duquel purger les tables de travail de la base de données. Utilisez cette option uniquement pour purger les tables de travail de la base de données lors de la suppression du service d'intégration de données. Cette option supprime définitivement toutes les lignes des tables de travail.

runMapping

Exécute un mappage qui est déployé vers un service d'intégration de données. Vous pouvez exécuter le mappage avec un paramètre défini ou un fichier de paramètres.

Pour créer un fichier de paramètres pour un mappage, exécutez la commande `infacmd ms listMappingParams`. Avant d'exécuter `infacmd ms listMappingParams`, exécutez la commande `infacmd dis startApplication` pour l'application.

Pour afficher les paramètres et les valeurs d'un ensemble de paramètres, exécutez la commande `infacmd dis listParameterSetEntries`.

La syntaxe de la commande `infacmd ms runMapping` est la suivante :

```
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]
```

La commande renvoie l'ID de tâche de l'exécution du mappage.

Vous devez activer la surveillance pour stocker le nom de l'instance d'exécution. Si vous purgez les statistiques de surveillance, les noms d'instance d'exécution sont supprimés et ne seront pas renvoyés par la commande `infacmd ms getMappingStatus`. Le journal de mappage peut encore contenir le nom de l'instance d'exécution et les sorties de mappage persistantes associées au nom de l'instance d'exécution peuvent encore être utilisées.

Le tableau suivant décrit les options et les arguments de la commande `infacmd ms runMapping` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui exécute le mappage. L'application qui contient le mappage doit être déployée dans un service d'intégration de données.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application_name	Requis. Nom de l'application qui contient le mappage.
-Mapping -m	mapping_name	Requis. Nom du mappage à exécuter.
-Wait -w	True False	Facultatif. Indique si la commande infacmd doit attendre que le mappage s'achève avant de retourner au shell ou à l'invite de commande. Si la valeur est True, la commande infacmd retourne au shell ou à l'invite de commande lorsque le mappage est terminé. Vous ne pouvez pas exécuter les commandes suivantes avant que le mappage ne soit terminé. Si la valeur est False, la commande infacmd retourne immédiatement au shell ou à l'invite de commande. Vous ne devez pas attendre que le mappage se termine pour exécuter la commande suivante. La valeur par défaut est False.
-ParameterFile -pf	parameter_file_path	Facultatif. Nom et chemin du fichier de paramètres. N'entrez pas un fichier de paramètres et un ensemble de paramètres.
-ParameterSet -ps	parameter_set_name	Facultatif. Nom d'un ensemble de paramètres à utiliser lors de l'exécution. L'option Ensemble de paramètres remplace n'importe quel ensemble de paramètres déployé avec l'application. N'entrez pas un ensemble de paramètres et un fichier de paramètres.

Option	Argument	Description
-OperatingSystemProfile -osp	operating_system_profile_name	Facultatif. Nom du profil de système d'exploitation pour l'exécution du mappage. Si vous n'utilisez pas cette option lorsque le service d'intégration de données est activé pour utiliser les profils du système d'exploitation, le service d'intégration de données exécute le mappage avec le profil par défaut.
-NodeName -nn	node_name	Facultatif. Nom du nœud dans une grille du service d'intégration de données sur lequel répartir la tâche de mappage. Un processus de service d'intégration de données doit être en cours d'exécution sur le nœud. Si vous n'utilisez pas cette option, la tâche de mappage est répartie sur le nœud sur lequel le processus du service d'intégration de données principal s'exécute.
-OptimizationLevel -ol	optimization_level	Facultatif. Contrôle les méthodes d'optimisation que le service d'intégration de données applique au mappage. Entrez la valeur numérique associée au niveau d'optimisation que vous voulez configurer. Entrez l'une des valeurs suivantes : -1 (Auto) Le service d'intégration de données applique les optimisations en fonction du mode d'exécution et des contenus de mappage. 0 (aucun) Le service d'intégration de données n'applique aucune optimisation. 1 (minimum) Le service d'intégration de données applique la méthode d'optimisation de projection précoce. 2 (normal) Le service d'intégration de données applique les méthodes d'optimisation de projection précoce, de sélection précoce, de nettoyage de branche, push-into, globale des prédicats et du prédicat. 3 (complet) Le service d'intégration de données applique les méthodes d'optimisation basée sur le coût, de projection précoce, de sélection précoce, de nettoyage de branche, de prédicat, push-into, de semi-jointure et de jointure dataship. La valeur par défaut est -1 (Auto).

Option	Argument	Description
-PushdownType -pt	pushdown_type	<p>Facultatif. Contrôle le type de refoulement que le service d'intégration de données applique à un mappage. Entrez l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> - Aucun. Aucun type de refoulement n'est sélectionné pour le mappage. - Source. Le service d'intégration de données tente de refouler le plus de logique de transformation possible vers la base de données source. - Complet. Le service d'intégration de données pousse la logique de transformation complète vers la base de données source. <p>Cette option remplace le type de refoulement défini dans les propriétés d'exécution du mappage ou dans un fichier ou un ensemble de paramètres.</p> <p>Si vous n'utilisez pas cette option, le service d'intégration de données applique le type de refoulement défini dans les propriétés d'exécution du mappage ou dans un fichier ou un ensemble de paramètres.</p>
-RuntimeInstanceName -rin	runtime_instance_name	<p>Facultatif. Nom de l'instance d'exécution du mappage. Le nom doit être unique.</p> <p>Le nom de l'instance d'exécution ne peut pas contenir de barres obliques.</p> <p>Vous devez spécifier un nom d'instance d'exécution dans runMapping pour persister les sorties de mappage et exécuter les commandes listMappingPersistedOutputs et deleteMappingPersistedOutputs.</p> <p>Astuce: Vous pouvez définir la valeur comme suit pour normaliser les noms d'instance d'exécution :</p> <ul style="list-style-type: none"> - Si tous les mappages d'une application utilisent les mêmes sorties de mappage persistantes, utilisez le nom de l'application. - Si les mappages utilisent des sorties de mappage persistantes différentes, utilisez une combinaison du nom de l'application, du nom de mappage et du nom de l'ensemble de paramètres ou de fichier.

Option	Argument	Description
-EnableAudit -ea	True False	Facultatif. Indique si les règles et conditions d'audit s'exécutent avec le mappage. La valeur par défaut est False. Cette option remplace la configuration Activer l'audit dans l'outil Developer tool. Par exemple, si vous sélectionnez Activer l'audit dans l'outil Developer tool et utilisez la valeur par défaut pour cette option, les règles et conditions d'audit ne s'exécutent pas.
-CustomProperties -cp	custom_properties	Facultatif. Définissez les propriétés personnalisées d'un mappage à la demande du support client international Informatica. Entrez les propriétés personnalisées en tant que paires nom-valeur séparées par des points-virgules. Par exemple : ... -cp custom_property_name=value Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

UpdateMappingOptions

Met à jour les options de mappage dans une application.

La syntaxe de la commande infacmd ms updateMappingOptions est la suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd ms updateMappingOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire. Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation. Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec ces deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui exécute le mappage. L'application qui contient le mappage doit être déployée dans un service d'intégration de données.
-Application -a	application_name	Requis. Nom de l'application qui contient le mappage.
-Mapping -m	mapping_name	Requis. Nom du mappage.
-Options -o	options	Facultatif. Liste des options à configurer. Séparez chaque option par un espace. Pour afficher des options, exécutez la commande infacmd as ListServiceOptions.

UpdateOptimizationDefaultLevel

Met à jour le niveau d'optimisation à -1 (Auto) pour tous les mappages d'une application avec le niveau d'optimisation 2 (Normal). Avant la version 10.4.0, Normal était le niveau d'optimisation par défaut. Auto est la valeur par défaut pour tous les nouveaux mappages. La commande n'affecte pas les mappages dans l'application avec un niveau d'optimisation autre que Normal.

La syntaxe de la commande infacmd ms updateOptimizationDefaultLevel est la suivante :

```

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

```

Le tableau suivant décrit les options et les arguments de la commande `infacmd ms updateOptimizationDefaultLevel` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui exécute le mappage. L'application qui contient le mappage doit être déployée dans un service d'intégration de données.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec ces deux méthodes, l'option -re est prioritaire.
-Application -a	application_name	Requis. Nom de l'application qui contient le ou les mappages.

UpdateOptimizationLevel

Met à jour le niveau d'optimisation de plusieurs mappages d'une application.

La commande infacmd ms updateOptimizationLevel utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd ms updateOptimizationLevel :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui exécute le mappage. L'application qui contient le mappage doit être déployée dans un service d'intégration de données.

Option	Argument	Description
-UserName -un	user_name	<p>Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>
-Password -pd	mot de passe	<p>Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p> <p>Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.</p>
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p> <p>Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec ces deux méthodes, l'option -re est prioritaire.</p>
-Application -a	application_name	<p>Requis. Nom de l'application qui contient le ou les mappages.</p>

Option	Argument	Description
-Mapping -m	mapping_name	Facultatif. Nom du mappage à modifier. Pour mettre à jour le niveau d'optimisation pour plusieurs mappages, séparez chaque nom de mappage par une virgule. La valeur par défaut est tous les mappages d'une application.
-OptimizationLevel -ol	optimization_level	Facultatif. La méthode d'optimisation que le service d'intégration de données applique à un mappage. Entrez l'une des valeurs suivantes : -1 (Auto) Le service d'intégration de données applique les optimisations en fonction du mode d'exécution et des contenus de mappage. 0 (aucun) Le service d'intégration de données n'applique aucune optimisation. 1 (minimum) Le service d'intégration de données applique la méthode d'optimisation de projection précoce. 2 (normal) Le service d'intégration de données applique les méthodes d'optimisation de projection précoce, de sélection précoce, de nettoyage de branche, push-into, globale des prédicats et du prédicat. 3 (complet) Le service d'intégration de données applique les méthodes d'optimisation basée sur le coût, de projection précoce, de sélection précoce, de nettoyage de branche, de prédicat, push-into, de semi-jointure et de jointure dataship. La valeur par défaut est -1 (Auto).

upgradeMappingParameterFile

Convertit un fichier de paramètre que vous avez créé dans une version précédente d'Informatica en un format de fichier de paramètre valide pour la version 10.0 d'Informatica.

Dans Informatica version 10.0, un fichier de paramètres peut contenir des paramètres de mappage et de flux de travail, mais il ne contient plus de paramètres de transformation. Lorsque vous exécutez un mappage ou un flux de travail avec la version précédente du fichier de paramètres, le service d'intégration de données doit convertir le fichier de paramètres pour la version Informatica 10.0 lors de l'exécution. Vous pouvez augmenter les performances en convertissant les fichiers de paramètres au format Informatica 10.0.

La commande `infacmd ms upgradeMappingParameterFile` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments d'`infacmd ms upgradeMappingParameterFile` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui exécute le mappage. L'application qui contient le mappage doit être déployée dans un service d'intégration de données.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire. Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p> <p>Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>
-Application -a	application_name	Requis. Nom de l'application qui contient le mappage.
-Mapping -m	mapping_name	Requis. Nom du mappage.
- OutputFile - o	sortie file_to_write_to	Facultatif. Chemin et nom du fichier de paramètres à créer. Si vous ne spécifiez pas de fichier, la commande affiche les paramètres dans l'invite de commande.
-ParameterFile -pf	parameter_file_to_upgrade	Requis. Nom du fichier de paramètre à mettre à niveau.

CHAPITRE 27

Référence de commande infacmd oie

Le plug-in oie est obsolète. Il ne sera plus pris en charge dans une version ultérieure. Les commandes infacmd oie ont été migrées vers le plug-in tools. Pour afficher les descriptions des commandes, consultez le [Chapitre 37, "Référence de commande infacmd tools" à la page 1172](#).

CHAPITRE 28

Référence de commande infacmd ps

Ce chapitre comprend les rubriques suivantes :

- [cancelProfileExecution, 962](#)
- [CreateWH, 964](#)
- [detectOrphanResults, 966](#)
- [DropWH, 967](#)
- [Exécuter, 969](#)
- [executeProfile, 971](#)
- [getExecutionStatus, 973](#)
- [getProfileExecutionStatus, 975](#)
- [Liste, 977](#)
- [ListAllProfiles, 979](#)
- [migrateProfileResults, 980](#)
- [migrateScorecards, 982](#)
- [Purger, 984](#)
- [purgeOrphanResults, 986](#)
- [restoreProfilesAndScorecards, 988](#)
- [synchronizeProfile, 990](#)

cancelProfileExecution

Interrompt toutes les exécutions de profils comprenant des profils et un profil de découverte des données d'entreprise.

La commande infacmd ps cancelProfileExecution utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et arguments d'infacmd ps cancelProfileExecution :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.
-NodeName -nn	node_name	Facultatif. Nom du nœud sur lequel s'exécute le service d'intégration de données.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-MrsServiceName -msn	MRS_name	Requis. Nom du service de référentiel modèle.
-DsServiceName -dsn	data_integration_service_name	Requis. Nom du service d'intégration de données.
-ObjectPathAndName -opn	MRS_object_path	Requis. Utilisez la syntaxe suivante : ProjectName/FolderName/.../SubFolder_Name/ {ObjectName ProjectName/ObjectName}

CreateWH

Crée le contenu de l'entrepôt de profilage.

La commande infacmd ps CreateWH utilise la syntaxe suivante :

```
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
```


Le tableau suivant décrit les options et arguments d'infacmd ps CreateWH :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-Gateway -hp	gateway_name	Facultatif. Utilisez cette option si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Entrez le nom d'hôte et le numéro de port pour le nœud de passerelle dans le domaine. Utilisez la syntaxe suivante : gateway_hostname:port.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire. Obligatoire. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation. Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.
-DsServiceName -dsn	data_integration_service_name	Obligatoire. Nom du service d'intégration de données.

detectOrphanResults

Détecte les résultats de profil dans l'entrepôt de profilage qui n'ont pas de profil associé à dans le référentiel modèle. Lorsque vous supprimez un profil avant de l'ouvrir, l'outil Developer ou l'outil Analyst supprime ce profil et ses métadonnées du référentiel modèle. Par conséquent, des résultats de profil se retrouvent orphelins dans l'entrepôt de profilage. Pour détecter les résultats de profil orphelins, vous pouvez exécuter la commande `infacmd ps detectOrphanResults`. Pour enregistrer la sortie de la commande dans un fichier, exécutez la commande `infacmd ps detectOrphanResults > <nomdufichier>`.

La commande `infacmd ps detectOrphanResults` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments de la commande `infacmd ps detectOrphanResults` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Le nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-Gateway -hp	gateway_name	Facultatif si vous exécutez la commande depuis le répertoire d'installation \bin d'Informatica. Obligatoire si vous exécutez la commande depuis un autre emplacement. Nom du nœud de passerelle. Utilisez la syntaxe suivante : [Domain_Host]:[HTTP_Port]
-NodeName -nn	node_name	Obligatoire. Nom du nœud où le service d'intégration de données s'exécute.

Option	Argument	Description
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	Mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-MrsServiceName -msn	MRS_name	Obligatoire. Le nom du service de référentiel modèle.
-DsServiceName -dsn	data_integratio n_service_name	Obligatoire. Nom du service d'intégration de données

DropWH

Supprime le contenu de l'entrepôt de profilage.

La commande infacmd ps DropWH utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et arguments d'infacmd ps DropWH :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-Gateway -hp	gateway_name	Facultatif. Utilisez cette option si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Entrez le nom d'hôte et le numéro de port pour le nœud de passerelle dans le domaine. Utilisez la syntaxe suivante : gateway_hostname:port.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire. Obligatoire. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p> <p>Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.</p>
-DsServiceName -dsn	data_integration_service_name	Obligatoire. Nom du service d'intégration de données.

Exécuter

Exécute un profil ou une fiche d'évaluation.

La commande infacmd ps Execute utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd ps Exécute :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-NodeName -nn	node_name	Facultatif. Nom du nœud sur lequel s'exécute le service d'intégration de données.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-MrsServiceName -msn	MRS_name	Requis. Nom du service de référentiel modèle.

Option	Argument	Description
-DsServiceName -dsn	data_inetgration_s service_name	Requis. Nom du service d'intégration de données.
-ObjectType -ot	object_type	Requis. Entrez un profil ou une fiche d'évaluation.
-ObjectPathandName -opn	MRS_object_path	Requis. Utilisez la syntaxe suivante : ProjectName/FolderName/.../SubFolder_Name/ {ObjectName ProjectName/ObjectName}
-ProfileName -pt	profile_task_name	Facultatif. Nom d'une tâche de profil dans le profil de découverte des données d'entreprise.
-Wait -w	True False	Facultatif. Si cette option est définie sur True, elle attend que la commande se termine avant de renvoyer l'invite de commande. Si elle est définie sur False, elle renvoie l'invite de commande avant la fin de la commande. La valeur par défaut est False.
-ospn -OsProfileName	os_profile_name	Facultatif. Nom du profil du système d'exploitation si le service d'intégration de données est activé pour utiliser les profils du système d'exploitation.

executeProfile

Exécute un profil de découverte des données d'entreprise.

La commande infacmd ps executeProfile utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd ps executeProfile :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-NodeName -nn	node_name	Facultatif. Nom du nœud sur lequel s'exécute le service d'intégration de données.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-MrsServiceName -msn	MRS_name	Requis. Nom du service de référentiel modèle.

Option	Argument	Description
-DsServiceName -dsn	data_inetgration_s ervice_name	Requis. Nom du service d'intégration de données.
-ObjectPathandName -opn	MRS_object_path	Requis. Utilisez la syntaxe suivante : ProjectName/FolderName/.../SubFolder_Name/ {ObjectName ProjectName/ObjectName}
-WaitForModelExecToFinish -w	True False	Facultatif. Si cette option est définie sur True, elle attend que la commande se termine avant de renvoyer l'invite de commande. Si elle est définie sur False, elle renvoie l'invite de commande avant la fin de la commande. La valeur par défaut est False.
-ospn -OsProfileName	os_profile_name	Facultatif. Nom du profil du système d'exploitation si le service d'intégration de données est activé pour utiliser les profils du système d'exploitation.

getExecutionStatus

Obtient le statut d'exécution des tâches de profil dans un profil de découverte des données d'entreprise.

La commande infacmd ps getExecutionStatus utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd ps getExecutionStatus :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.
-NodeName -nn	node_name	Facultatif. Nom du nœud sur lequel s'exécute le service d'intégration de données.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-MrsServiceName -msn	MRS_name	Requis. Nom du service de référentiel modèle.

Option	Argument	Description
-DsServiceName -dsn	data_integration_service_name	Requis. Nom du service d'intégration de données.
-ObjectType -ot	object_type	Requis. Entrez un profil ou une fiche d'évaluation.
-ObjectPathAndName -opn	MRS_object_path	Requis. Utilisez la syntaxe suivante : ProjectName/FolderName/.../SubFolder_Name/ {ObjectName ProjectName/ObjectName}
-ProfileTaskName -pt	profile_task_name	Facultatif. Nom d'une tâche de profil dans le profil de découverte des données d'entreprise.

getProfileExecutionStatus

Obtient le statut d'exécution d'un profil de découverte des données d'entreprise. La commande répertorie également toutes les tâches de profil dans le profil de découverte des données d'entreprise ainsi que leurs statuts d'exécution.

La commande infacmd ps getProfileExecutionStatus utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd ps getProfileExecutionStatus :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.
-NodeName -nn	node_name	Facultatif. Nom du nœud sur lequel s'exécute le service d'intégration de données.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-MrsServiceName -msn	MRS_name	Requis. Nom du service de référentiel modèle.

Option	Argument	Description
-DsServiceName -dsn	data_integration_service_name	Requis. Nom du service d'intégration de données.
-ObjectPathAndName -opn	MRS_object_path	Requis. Utilisez la syntaxe suivante : ProjectName/FolderName/.../SubFolder_Name/ {ObjectName ProjectName/ObjectName}

Liste

Répertorie les profils ou les fiches d'évaluation.

La commande infacmd ps List utilise la syntaxe suivante :

```
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>]
```

Le tableau suivant décrit les options et arguments d'infacmd ps List :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-NodeName -nn	node_name	Facultatif. Nom du nœud sur lequel s'exécute le service d'intégration de données.

Option	Argument	Description
-MrsServiceName -msn	MRS_name	Requis. Nom du service de référentiel modèle.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ObjectType -ot	-	Requis. Entrez un profil ou une fiche d'évaluation.
-FolderPath -fp	full_folder_path	Requis. Entrez le chemin d'accès du dossier contenant les objets à répertorier. Utilisez la syntaxe suivante : Project_name/folder_name/../../SubFolderName
-Recursive -r	-	Facultatif. Applique la commande aux objets situés dans le dossier que vous spécifiez et dans ses sous-dossiers.

ListAllProfiles

Répertorie tous les profils d'un profil de découverte d'entreprise.

La commande infacmd ps ListAllProfiles utilise la syntaxe suivante :

```
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>
```

Le tableau suivant décrit les options et arguments de la commande infacmd ps ListAllProfiles :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-NodeName -nn	node_name	Facultatif. Nom du nœud sur lequel s'exécute le service d'intégration de données.
-MrsServiceName -msn	MRS_name	Requis. Nom du service de référentiel modèle.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ProfilePathAndName -pn	profile_path_and_name	Requis. Entrez le chemin d'accès au profil de découverte d'entreprise et son nom.

migrateProfileResults

Migre les résultats du profil de colonne et de la découverte de domaines de données depuis la version 9.1.0, 9.5.0 ou 9.5.1.

La commande `infacmd ps migrateProfileResults` utilise la syntaxe suivante :

```
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
```


Le tableau suivant décrit les options et arguments d'infacmd ps migrateProfileResults :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-NodeName -nn	node_name	Facultatif. Nom du nœud où le service d'intégration de données s'exécute.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-MrsServiceName -msn	MRS_name	Obligatoire. Nom du service de référentiel modèle.
-DsServiceName -dsn	data_integration_s service_name	Obligatoire. Nom du service d'intégration de données.

migrateScorecards

Migre les résultats de fiche d'évaluation depuis Informatica 9.1.0 ou 9.5.0 vers 9.5.1.

La commande `infacmd ps migrateScorecards` utilise la syntaxe suivante :

```

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

```

Le tableau suivant décrit les options et arguments d'`infacmd ps migrateScorecards` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-NodeName -nn	node_name	Facultatif. Nom du nœud sur lequel s'exécute le service d'intégration de données.

Option	Argument	Description
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-MrsServiceName -msn	MRS_name	Requis. Nom du service de référentiel modèle.
-DsServiceName -dsn	data_integration_service_name	Requis. Nom du service d'intégration de données.
-migrateFrom -mfr	migrate_from_release	Requis. Version de l'explorateur de données à partir de laquelle s'effectue la migration. La version peut être 9.1.0 ou 9.5.0. Si vous avez exécuté des profils et des fiches d'évaluation dans les versions 9.0, 9.0.1 ou 9.1.0, entrez la valeur 9.1.0. Si vous avez exécuté des profils et des fiches d'évaluation dans la version 9.5.0, entrez la valeur 9.5.0.

Purger

Purge les résultats de profil ou de fiche d'évaluation de l'entrepôt de profilage. La commande `infacmd ps Purge` purge tous les résultats de profil et de fiche d'évaluation, à l'exception des résultats de la dernière exécution du profil ou de la fiche d'évaluation.

La commande `infacmd ps Purge` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'`infacmd ps Purge` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Le nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-Gateway -hp	gateway_name	Facultatif si vous exécutez la commande depuis le répertoire d'installation \bin d'Informatica. Requis si vous exécutez la commande depuis un autre emplacement. Nom du nœud de passerelle. Utilisez la syntaxe suivante : [Domain_Host]:[HTTP_Port]
-NodeName -nn	node_name	Requis. Nom du nœud où le service d'intégration de données s'exécute.

Option	Argument	Description
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	Mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-MrsServiceName -msn	MRS_name	Requis. Le nom du service de référentiel modèle.
-DsServiceName -dsn	data_integratio n_service_name	Requis. Nom du service d'intégration de données
-ObjectType -ot	-	Requis. Entrez un profil ou une fiche d'évaluation.
-ObjectPathAndName -opn *	MRS_object_path	Facultatif. Ne pas utiliser avec ProjectFolderPath ou Recursive. Chemin d'accès au profil ou à la fiche d'évaluation dans le référentiel modèle. Utilisez la syntaxe suivante : ProjectName/FolderName/.../{SubFolder_Name/ObjectName ProjectName/ObjectName}

Option	Argument	Description
-RetainDays -rd	results_retain_days	Facultatif. Spécifie la plage de temps des résultats du profil et de la fiche d'évaluation afin d'être admissibles pour la rétention dans l'entrepôt de profilage. Le service d'intégration de données purge le reste des résultats de profil et de fiche d'évaluation. Par exemple, si vous entrez -rd 10, les résultats du jour en cours et des neuf derniers jours sont conservés et les autres résultats sont purgés de l'entrepôt de profilage.
-ProjectFolderPath -pf *	project_folder_path	Facultatif. Ne pas utiliser avec ObjectPathAndName ou ProfileTaskName. Noms du projet et du dossier dans lesquels le profil ou la fiche d'évaluation sont stockés. Utilisez la syntaxe suivante : ProjectName/FolderName
-ProfileName -pt *	profile_task_name	Facultatif. Nom de la tâche de profil que vous voulez purger. Si un dossier n'a qu'un seul profil, vous pouvez utiliser uniquement l'option ProjectFolderPath, car ProjectFolderPath inclut le nom du profil qui contient la tâche de profil. Si un dossier comporte plusieurs profils, utilisez l'option ProfileName avec l'option ProjectFolderPath pour spécifier le nom du profil.
-Recursive -r	recursive	Facultatif. Ne pas utiliser avec ObjectPathAndName. Applique la commande aux objets situés dans le dossier que vous spécifiez et dans ses sous-dossiers.
-PurgeAllResults -pa	purge_all_results	Facultatif. Définissez cette option pour purger tous les résultats de l'objet de la fiche d'évaluation ou du profil. Utilisez-la avec l'option -recursive pour appliquer la commande aux résultats de fiche d'évaluation ou de profil dans le dossier que vous spécifiez et dans ses sous-dossiers.
* Pour exécuter la commande, vous devez spécifier ObjectPathAndName, ProjectFolderPath ou ProfileTaskName.		

purgeOrphanResults

Purge les résultats de profil orphelins de l'entrepôt de profilage. Vous pouvez exécuter cette commande après avoir exécuté la commande `infacmd ps detectOrphanResults` pour détecter les résultats de profil orphelins.

La commande `infacmd ps purgeOrphanResults` utilise la syntaxe suivante :

```

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

```

Le tableau suivant décrit les options et arguments de la commande `infacmd ps purgeOrphanResults` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Le nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-Gateway -hp	gateway_name	Facultatif si vous exécutez la commande depuis le répertoire d'installation \bin d'Informatica. Obligatoire si vous exécutez la commande depuis un autre emplacement. Nom du nœud de passerelle. Utilisez la syntaxe suivante : [Domain_Host]:[HTTP_Port]
-NodeName -nn	node_name	Obligatoire. Nom du nœud où le service d'intégration de données s'exécute.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	Mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-MrsServiceName -msn	MRS_name	Obligatoire. Le nom du service de référentiel modèle.
-DsServiceName -dsn	data_integration_service_name	Obligatoire. Nom du service d'intégration de données
-filePathName -fpn	filePathName	Obligatoire. Chemin d'accès et nom du fichier qui contient une liste des ID de profil. Les ID de profil sont mappés aux résultats de profil orphelins qui doivent être purgés.

restoreProfilesAndScorecards

Restaure les profils et les fiches d'évaluation d'une version précédente vers la version actuelle.

Parfois, une fois que vous avez mis à niveau et analysé en détail les résultats de profil existants ou les résultats de fiches d'évaluation, il est possible que les colonnes de règles n'apparaissent pas dans les résultats détaillés. Pour inclure des colonnes de règles dans les résultats, exécutez la commande `infacmd ps restoreProfilesAndScorecards`. Assurez-vous d'avoir créé une sauvegarde du contenu du référentiel modèle avant d'exécuter la commande.

La commande `infacmd ps restoreProfilesAndScorecards` utilise la syntaxe suivante :

```
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
```


Le tableau suivant décrit les options et arguments de la commande `infacmd ps restoreProfilesAndScorecards` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Le nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-Gateway -hp	gateway_name	Facultatif si vous exécutez la commande depuis le répertoire d'installation <code>\bin d\Informatica</code> . Requis si vous exécutez la commande depuis un autre emplacement. Nom du nœud de passerelle. Utilisez la syntaxe suivante : <code>[Domain_Host]:[HTTP_Port]</code>
-NodeName -nn	node_name	Requis. Nom du nœud où le service d'intégration de données s'exécute.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	Mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-MrsServiceName -msn	MRS_name	Requis. Le nom du service de référentiel modèle.
-DsServiceName -dsn	data_integratio n_service_nam e	Requis. Nom du service d'intégration de données.

synchronizeProfile

Migre les clés primaires et étrangères documentées, définies par l'utilisateur et validées pour tous les profils d'un projet depuis la version 9.1.0, 9.5.0 ou 9.5.1.

La commande infacmd ps synchronizeProfile utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd ps synchronizeProfile :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si les informations de connectivité de passerelle dans le fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-NodeName -nn	node_name	Facultatif. Nom du nœud où le service d'intégration de données s'exécute.

Option	Argument	Description
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-MrsServiceName -msn	MRS_name	Obligatoire. Nom du service de référentiel modèle.
-DsServiceName -dsn	data_integration_service_name	Obligatoire. Nom du service d'intégration de données.
-ProjectName -pn	project_name	Obligatoire. Nom du projet.

CHAPITRE 29

Référence de commande infacmd pwx

Ce chapitre comprend les rubriques suivantes :

- [CloseForceListener, 993](#)
- [CloseListener, 995](#)
- [CondenseLogger, 998](#)
- [createdatamaps, 1000](#)
- [CreateListenerService, 1003](#)
- [CreateLoggerService, 1006](#)
- [DisplayAllLogger, 1010](#)
- [DisplayCPULogger, 1013](#)
- [DisplayEventsLogger, 1015](#)
- [DisplayMemoryLogger, 1018](#)
- [DisplayRecordsLogger, 1020](#)
- [displayStatsListener, 1024](#)
- [DisplayStatusLogger, 1027](#)
- [FileSwitchLogger, 1030](#)
- [ListTaskListener, 1032](#)
- [ShutDownLogger, 1035](#)
- [StopTaskListener, 1038](#)
- [UpgradeModels, 1041](#)
- [UpdateListenerService, 1043](#)
- [UpdateLoggerService, 1046](#)

CloseForceListener

Force l'annulation des sous-tâches de longue durée sur l'Ecouteur PowerExchange et interrompt le service d'écoute.

Lorsque vous exécutez la commande `infacmd pwx CloseForceListener`, PowerExchange effectue les actions suivantes :

1. Vérifie si des sous-tâches sont actives sur le service d'écoute.
2. Si des sous-tâches actives existent, elle recherche le nombre de sous-tâches actives chaque seconde, pendant 30 secondes.
3. Pendant cette période, elle interrompt toutes les sous-tâches qui attendent une entrée réseau TCP/IP.
4. Annule toutes les sous-tâches actives restantes.
5. Interrompt le service d'écoute.

La commande `infacmd pwx CloseForceListener` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'`infacmd pwx CloseForceListener` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	<p>Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>

Option	Argument	Description
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'écoute.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel la commande infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infra sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.

Option	Argument	Description
-OSUser -oun	OS_user_name	<p>Obligatoire si vous activez la sécurité du système d'exploitation. Nom d'utilisateur pour le système d'exploitation.</p> <p>Activez la sécurité du système d'exploitation comme suit :</p> <ul style="list-style-type: none"> - Pour imposer aux utilisateurs de fournir dans la commande un identifiant et un mot de passe utilisateur du système d'exploitation valides, spécifiez 1 ou 2 dans le premier paramètre de l'instruction SECURITY dans le fichier de configuration DBMOVER sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange utilise les fonctions du système d'exploitation du système cible pour authentifier l'identifiant et le mot de passe utilisateur pour l'utilisation du programme infacmd pwx. - Pour autoriser les utilisateurs à exécuter des commandes infacmd pwx, spécifiez 2 dans le premier paramètre de l'instruction SECURITY et définissez les instructions AUTHGROUP et USER dans le fichier sign-on PowerExchange sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange vérifie le fichier Sign-On pour déterminer si l'identifiant utilisateur fourni est autorisé à exécuter des commandes dans le programme infacmd pwx. <p>Pour plus d'informations, consultez le <i>Manuel de référence PowerExchange</i>.</p>
-OSPassword -oup	OS_password	<p>Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe crypté. Mot de passe pour le système d'exploitation.</p> <p>Vous pouvez définir un mot de passe en texte clair avec l'option -p ou avec la variable d'environnement INFA_DEFAULT_PWX_OSPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -p est prioritaire.</p>
-OSEPassword -ouep	OS_epassword	<p>Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe en texte clair. Mot de passe crypté pour le système d'exploitation.</p> <p>Vous pouvez définir un mot de passe crypté avec l'option -e ou la variable d'environnement INFA_DEFAULT_PWX_OSEPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -e est prioritaire.</p>

CloseListener

Interrompt l'Ecouteur PowerExchange après avoir attendu que toutes les sous-tâches en attente sur le service d'écoute soient terminées.

Remarque: Si vous avez des sous-tâches de longue durée sur le service d'écoute, exécutez la commande infacmd pwx closeforceListener pour forcer l'annulation de toutes les sous-tâches utilisateur et arrêter le service d'écoute.

La commande `infacmd pwx CloseListener` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'`infacmd pwx CloseListener` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'écoute.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel la commande infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.
-OSUser -oun	OS_user_name	Obligatoire si vous activez la sécurité du système d'exploitation. Nom d'utilisateur pour le système d'exploitation. Activez la sécurité du système d'exploitation comme suit : <ul style="list-style-type: none"> - Pour imposer aux utilisateurs de fournir dans la commande un identifiant et un mot de passe utilisateur du système d'exploitation valides, spécifiez 1 ou 2 dans le premier paramètre de l'instruction SECURITY dans le fichier de configuration DBMOVER sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange utilise les fonctions du système d'exploitation du système cible pour authentifier l'identifiant et le mot de passe utilisateur pour l'utilisation du programme infacmd pwx. - Pour autoriser les utilisateurs à exécuter des commandes infacmd pwx, spécifiez 2 dans le premier paramètre de l'instruction SECURITY et définissez les instructions AUTHGROUP et USER dans le fichier sign-on PowerExchange sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange vérifie le fichier Sign-On pour déterminer si l'identifiant utilisateur fourni est autorisé à exécuter des commandes dans le programme infacmd pwx.

Option	Argument	Description
-OSPassword -oup	OS_password	Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe crypté. Mot de passe pour le système d'exploitation. Vous pouvez définir un mot de passe en texte clair avec l'option -p ou avec la variable d'environnement INFA_DEFAULT_PWX_OSPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -p est prioritaire.
-OSEPassword -ouep	OS_epassword	Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe en texte clair. Mot de passe crypté pour le système d'exploitation. Vous pouvez définir un mot de passe crypté avec l'option -e ou la variable d'environnement INFA_DEFAULT_PWX_OSEPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -e est prioritaire.

CondenseLogger

Démarre un autre cycle de journalisation avant la fin de la période d'attente pour le démarrage d'un autre cycle, quand le service de journalisation PowerExchange est exécuté en mode continue. Spécifiez la période d'attente dans le paramètre NO_DATA_WAIT du fichier de configuration pwxcl.cfg.

La commande infacmd pwx CondenseLogger utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd pwx CondenseLogger :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de journalisation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel la commande infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.

Option	Argument	Description
-OSUser -oun	OS_user_name	<p>Obligatoire si vous activez la sécurité du système d'exploitation. Nom d'utilisateur pour le système d'exploitation.</p> <p>Activez la sécurité du système d'exploitation comme suit :</p> <ul style="list-style-type: none"> - Pour imposer aux utilisateurs de fournir dans la commande un identifiant et un mot de passe utilisateur du système d'exploitation valides, spécifiez 1 ou 2 dans le premier paramètre de l'instruction SECURITY dans le fichier de configuration DBMOVER sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange utilise les fonctions du système d'exploitation du système cible pour authentifier l'identifiant et le mot de passe utilisateur pour l'utilisation du programme infacmd pwx. - Pour autoriser les utilisateurs à exécuter des commandes infacmd pwx, spécifiez 2 dans le premier paramètre de l'instruction SECURITY et définissez les instructions AUTHGROUP et USER dans le fichier sign-on PowerExchange sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange vérifie le fichier Sign-On pour déterminer si l'identifiant utilisateur fourni est autorisé à exécuter des commandes dans le programme infacmd pwx.
-OSPassword -oup	OS_password	<p>Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe crypté. Mot de passe pour le système d'exploitation.</p> <p>Vous pouvez définir un mot de passe en texte clair avec l'option -p ou avec la variable d'environnement INFA_DEFAULT_PWX_OSPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -p est prioritaire.</p>
-OSEPassword -ouep	OS_epassword	<p>Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe en texte clair. Mot de passe crypté pour le système d'exploitation.</p> <p>Vous pouvez définir un mot de passe crypté avec l'option -e ou la variable d'environnement INFA_DEFAULT_PWX_OSEPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -e est prioritaire.</p>

createdatamaps

Crée les cartes de données pour les opérations de mouvement de données en bloc.

Utilisez la commande createdatamaps pour générer des cartes de données pour les sources de données IMS, SEQ et VSAM depuis la ligne de commande. Cette commande fournit une alternative à l'utilisation du navigateur PowerExchange dans certains cas et vous permet de générer ou de régénérer des cartes de données de manière non interactive.

Si la commande échoue et renvoie une erreur de mémoire Java, augmentez la mémoire système disponible pour infacmd. Pour augmenter la mémoire système, définissez la valeur -Xmx dans la variable d'environnement ICMD_JAVA_OPTS. Pour plus d'informations, voir ["ICMD_JAVA_OPTS" à la page 46](#).

La commande infacmd pwx createdatamaps utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande infacmd pwx createdatamaps :

Option	Argument	Description
-pwxLocation -loc	pwx_location	Facultatif. Emplacement de la source de données comme spécifié dans une instruction NODE dans le fichier de configuration dbmover de PowerExchange. Si pwxLocation n'est pas spécifié, l'utilitaire createdatamaps accède les accès au copybook et aux métadonnées de la DBD sur le système de fichiers local. Si vous configurez le fichier de contrôle pour trouver les ID d'enregistrement, pwxLocation est requis.
-pwxUserName -pun	pwx_user_name	Facultatif. Identifiant utilisateur pour la connexion à l'écouteur PowerExchange, si pwxLocation est spécifié.

Option	Argument	Description
-pwxPassword -ppd	pwx_password	<p>Facultatif. Mot de passe pour la connexion à l'écouteur PowerExchange, si pwxLocation est spécifié.</p> <p>Au lieu d'un mot de passe, vous pouvez entrer une phrase de passe PowerExchange valide. Les phrases de passe pour accéder à un écouteur PowerExchange sur z/OS peuvent comporter de 9 à 128 caractères et contenir les caractères suivants :</p> <ul style="list-style-type: none"> - Lettres majuscules et minuscules - Numéros de 0 à 9 - Espaces - Les caractères spéciaux suivants : ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Remarque: Le premier caractère est une apostrophe.</p> <p>Les phrases secrètes ne peuvent pas inclure de guillemets simples ('), de guillemets doubles (") ou de symboles de devises.</p> <p>Si une phrase secrète contient des espaces, vous devez la placer entre guillemets doubles ("), par exemple, "Ceci est un exemple de phrase secrète". Si une phrase secrète contient des caractères spéciaux, vous devez l'encadrer par trois guillemets doubles ("""), par exemple, """"Cette phrase secrète contient des caractères spéciaux ! % & *.""". Si une phrase secrète contient uniquement des caractères alphanumériques sans espaces, vous pouvez l'entrer sans délimiteurs.</p> <p>Remarque: Sur z/OS, une phrase secrète RACF valide peut comporter jusqu'à 100 caractères. PowerExchange tronque les phrases de passe de plus de 100 caractères lorsqu'elles sont transmises à RACF pour la validation.</p> <p>Pour utiliser les phrases secrètes, vérifiez que le service d'écoute PowerExchange est exécuté avec une valeur supérieure ou égale à (1, N) pour le paramètre de sécurité SECURITY dans le membre DBMOVER. Pour plus d'informations, voir la section du <i>Manuel de référence PowerExchange</i> relative à l'instruction SECURITY.</p>
-pwxEncryptedPassword -epwd	pwx_encrypted_password	<p>Facultatif. Mot de passe crypté pour la connexion à l'écouteur PowerExchange, si pwxLocation est spécifié.</p> <p>Si l'écouteur PowerExchange s'exécute sur un système z/OS ou i5/OS, vous pouvez entrer une phrase de passe PowerExchange cryptée au lieu d'un mot de passe crypté. Ne cryptez pas une phrase de passe contenant des caractères qui ne sont pas valides, comme par exemple des guillemets doubles, des guillemets simples ou des symboles de devises.</p>
-datamapOutputDir -dod	datamap_output_directory	<p>Facultatif. Répertoire du fichier local dans lequel écrire les cartes de données de sortie. Le répertoire par défaut est le répertoire de travail actuel.</p>

Option	Argument	Description
-replace -r	replace_existing_datamaps	Facultatif. Spécifie s'il faut remplacer les cartes de données existantes. Si replace=Y, remplace tous les cartes de données dans datamap_output_directory qui ont le même nom que les cartes de données que vous créez. Si replace=N, ignore la création d'une carte de données si une carte de données portant le même nom existe déjà dans datamap_output_directory. La valeur par défaut est N.
-controlFile -cf	file_path_for_control_file	Requis. Chemin et nom du fichier de contrôle qui contrôle la génération de carte de données.
-logFile -lf	file_path_for_log_file	Facultatif. Chemin et nom du fichier journal de sortie. La valeur par défaut est STDOUT.
-verbosity -v	logging_verbosity	Facultatif. Commentaires pour les fichiers journaux. La valeur par défaut est INFO. Valeurs valides : <ul style="list-style-type: none"> - DEBUG. Journalisation plus détaillée. Peut afficher des traces de la pile. - INFO. Messages d'information. - WARN. Indique un problème potentiel. - ERROR. Indique un échec. Le traitement continue. - FATAL. Indique une condition fatale. Le processus se ferme.

Le nom du nœud PowerExchange et les justificatifs d'identité sont facultatifs. Si vous n'incluez pas l'option pwxLocation, la commande accède au système de fichiers local directement pour lire les métadonnées. Dans ce cas, PowerExchange n'a pas besoin d'être installé sur la machine sur laquelle vous exécutez createdatamaps.

Pour plus d'informations sur la commande createdatamaps, consultez le *Guide des utilitaires PowerExchange*.

CreateListenerService

Crée un Ecouteur PowerExchange dans un domaine. Par défaut, le service d'écoute est désactivé lorsque vous le créez. Exécutez la commande infacmd isp EnableService pour activer le service.

La commande infacmd pwx CreateListenerService utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et arguments d'infacmd pwx CreateListenerService :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Obligatoire si -DomainName n'est pas spécifié. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.

Option	Argument	Description
ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'écoute. Le nom n'est pas sensible à la casse. Le nom ne peut pas dépasser 128 caractères ou contenir des retours chariot, des tabulations, des espaces ou les caractères suivants : / * ? < > "
-NodeName -nn	node_name	Requis. Nom du nœud sur lequel vous souhaitez que le service d'écoute s'exécute.
-LicenseName -ln	license_name	Facultatif. Licence à attribuer au service. Si vous ne sélectionnez pas une licence tout de suite, vous pourrez en attribuer une au service ultérieurement. Obligatoire avant d'activer le service.
-BackupNode -bn	backup_node	Facultatif. Si l'environnement PowerCenter est configuré pour une haute disponibilité, cette option spécifie le nom du nœud de sauvegarde.
-StartParameters -sp	start_parameters	Paramètres à inclure lorsque vous démarrez le service d'écoute. Séparez les paramètres par un espace. Le paramètre <i>node_name</i> est obligatoire. Vous pouvez inclure les paramètres suivants : - <i>node_name</i> Requis. Nom du nœud qui identifie le service d'écoute. Ce nom doit correspondre à celui de l'instruction LISTENER dans le fichier de configuration DBMOVER. - <i>config=directory</i> Facultatif. Spécifie le chemin d'accès complet et le nom de fichier de tout fichier de configuration à préférer au fichier dbmover.cfg par défaut. Cet autre fichier de configuration est prioritaire sur tout fichier de configuration spécifié dans la variable d'environnement PWX_CONFIG. - <i>license=directory/license_key_file</i> Facultatif. Spécifie le chemin d'accès complet et le nom de tout fichier de clé de licence à préférer au fichier license.key par défaut. Le nom ou le chemin d'accès du fichier de clé de licence de substitution doit différer de celui du fichier par défaut. Cet autre fichier de clé de licence est prioritaire sur tout fichier de clé de licence spécifié dans la variable d'environnement PWX_LICENSE. Remarque: Dans les paramètres config et license, vous devez indiquer le chemin d'accès complet uniquement si le fichier ne se trouve pas dans le répertoire d'installation. Placez les chemins d'accès et les noms de fichier qui contiennent des espaces entre guillemets.
-SvcPort -vp	service_port	Requis. Port sur lequel le service d'écoute surveille les commandes émises par le gestionnaire de service.

CreateLoggerService

Crée un service de journalisation PowerExchange dans un domaine. Par défaut, le service de journalisation est désactivé lorsque vous le créez. Exécutez la commande `infacmd isp EnableService` pour activer le service.

La commande `infacmd pwx CreateLoggerService` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'`infacmd pwx CreateLoggerService` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port...	Facultatif. Si -DomainName n'est pas spécifié. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	<p>Requis. Nom du service de journalisation.</p> <p>Le nom n'est pas sensible à la casse. Le nom ne peut pas dépasser 128 caractères ou contenir des retours chariot, des tabulations, des espaces ou les caractères suivants :</p> <p>/ * ? < > " </p>
-NodeName -nn	node_name	Requis. Nom du nœud sur lequel vous souhaitez que le service de journalisation s'exécute.
-LicenseName -ln	license_name	Facultatif. Licence à attribuer au service. Si vous ne sélectionnez pas une licence tout de suite, vous pourrez en attribuer une au service ultérieurement. Obligatoire avant d'activer le service.
-BackupNode -bn	backup_node	Facultatif. Si l'environnement PowerCenter est configuré pour une haute disponibilité, cette option spécifie le nom du nœud de sauvegarde.

Option	Argument	Description
-StartParameters -sp	start_parameters	<p>Facultatif. Paramètres à inclure lorsque vous démarrez le service de journalisation. Séparez les paramètres par un espace.</p> <p>Vous pouvez inclure les paramètres suivants :</p> <ul style="list-style-type: none"> - coldstart={Y N} Indique si le service de journalisation doit être démarré à froid ou à chaud. Entrez Y pour démarrer le service de journalisation à froid. Si le fichier CDCT contient des enregistrements de journaux, le service de journalisation les supprime. Entrez N pour démarrer le service de journalisation à chaud à partir du point de redémarrage indiqué dans le fichier CDCT. La valeur par défaut est N. - config=directory/pwx_config_file Spécifie le chemin d'accès complet et le nom de fichier de tout fichier de configuration à préférer au fichier dbmover.cfg par défaut. Cet autre fichier de configuration est prioritaire sur tout fichier de configuration spécifié dans la variable d'environnement PWX_CONFIG. - cs=directory/pwxlogger_config_file Spécifie le chemin d'accès et le nom du fichier de configuration du service de journalisation. Vous pouvez également utiliser le paramètre cs pour indiquer un fichier de configuration du service de journalisation qui remplace le fichier pwxcl.cfg par défaut. Le nom ou le chemin d'accès du fichier de substitution doit différer de celui du fichier par défaut. - encryptepwd=encrypted_password Mot de passe au format crypté qui permet d'activer le cryptage des fichiers journaux du service de journalisation PowerExchange. Avec ce mot de passe, le service de journalisation PowerExchange peut générer une clé de cryptage unique pour chaque fichier journal du service. Le mot de passe est stocké dans le fichier CDCT au format crypté. Pour des raisons de sécurité, le mot de passe n'est pas stocké dans des fichiers de sauvegarde CDCT et n'est pas affiché dans les rapports CDCT que vous pouvez générer avec l'utilitaire PWXUCDCT de PowerExchange. Si vous définissez ce paramètre, vous devez également définir coldstart sur Y. Si vous définissez ce paramètre, mais définissez également le paramètre ENCRYPTEPWD dans le fichier de configuration du service de journalisation PowerExchange (pwxcl.cfg), le paramètre défini dans le fichier de configuration est prioritaire. Si vous définissez ce paramètre ainsi que le paramètre ENCRYPTEPWD dans le fichier de configuration du service de journalisation PowerExchange, une erreur se produit. Vous pouvez définir l'algorithme AES à utiliser pour le cryptage du fichier journal dans le paramètre ENCRYPTOPT du fichier pwxcl.cfg. La valeur par défaut est AES128. Astuce: pour optimiser la sécurité, Informatica recommande de spécifier le mot de passe de cryptage lors du démarrage à froid du service de journalisation PowerExchange, plutôt que de le spécifier dans le fichier de configuration pwxcl.cfg. Cette pratique peut réduire les risques d'accès malveillant au

Option	Argument	Description
		<p>mot de passe de cryptage pour les raisons suivantes : 1) Le mot de passe de cryptage n'est pas stocké dans le fichier pwxcl.cfg. 2) Vous pouvez supprimer le mot de passe de la ligne de commande après le démarrage à froid. Si vous spécifiez le cryptage de mot de passe pour un démarrage à froid et que vous devez restaurer le fichier CDCT par la suite, vous devez entrer le même mot de passe de cryptage dans la commande RESTORE_CDCT de l'utilitaire PWXUCDCT.</p> <p>Pour <i>ne pas</i> crypter les fichiers journaux du service de journalisation PowerExchange, n'entrez pas de mot de passe de cryptage.</p> <ul style="list-style-type: none"> - <code>license=directory/license_key_file</code> Spécifie le chemin d'accès complet et le nom de tout fichier de clé de licence à préférer au fichier license.key par défaut. Le nom ou le chemin d'accès du fichier de clé de licence de substitution doit différer de celui du fichier par défaut. Cet autre fichier de clé de licence est prioritaire sur tout fichier de clé de licence spécifié dans la variable d'environnement PWX_LICENSE. - <code>specialstart={Y N}</code> Indique si vous effectuez un démarrage spécial pour le service de journalisation PowerExchange. Un démarrage spécial commence par un processus de capture de PowerExchange à partir du point du flux de modifications que vous spécifiez dans le fichier pwxcl.cfg. Ce point de démarrage remplace le point de redémarrage défini dans le fichier CDCT pour l'exécution du service de journalisation PowerExchange. Un démarrage spécial ne supprime aucun contenu du fichier CDCT. Utilisez ce paramètre pour ignorer les sections problématiques dans les journaux sources sans perdre les données capturées. Par exemple, utilisez le démarrage spécial dans les cas suivants : <ul style="list-style-type: none"> - Vous ne souhaitez pas que le service de journalisation PowerExchange capture la mise à niveau d'un catalogue Oracle. Dans ce cas, arrêtez le service de journalisation PowerExchange avant la mise à niveau. Une fois la mise à niveau terminée, générez une nouvelle séquence et des jetons de redémarrage pour le service de journalisation PowerExchange selon le SCN après la mise à niveau. Entrez la valeur de ces jetons dans les paramètres SEQUENCE_TOKEN et RESTART_TOKEN du fichier pwxcl.cfg, puis effectuez un démarrage spécial du service de journalisation PowerExchange. - Vous ne souhaitez pas que le service de journalisation PowerExchange traite à nouveau les journaux anciens et indisponibles provoqués par des unités de travail en cours non pertinentes pour CDC. Dans ce cas, arrêtez le service de journalisation PowerExchange. Modifiez la valeur RESTART_TOKEN de manière à refléter la valeur SCN du journal le plus récent disponible, puis effectuez un démarrage spécial. Si l'une des unités de travail en cours ayant démarré avant ce point de redémarrage est pertinente pour CDC, des données peuvent être perdues. <p>Valeurs valides :</p> <ul style="list-style-type: none"> - Y. Effectuez un démarrage spécial du service de journalisation PowerExchange depuis le point du flux de

Option	Argument	Description
		<p>modifications défini dans les valeurs des paramètres SEQUENCE_TOKEN et RESTART_TOKEN dans le fichier de configuration pwxcl.cfg. Vous devez spécifier des valeurs de jetons valides dans le fichier pwxcl.cfg. pour effectuer un démarrage spécial. Ces valeurs de jeton remplacent celles du fichier CDCT. Vérifiez que la valeur SEQUENCE_TOKEN dans le fichier pwxcl.cfg est supérieure ou égale à celle du jeton de la séquence actuelle dans le fichier CDCT.</p> <p>Enfin, ne définissez pas le paramètre coldstart sur Y. Sinon, ce paramètre devient prioritaire.</p> <ul style="list-style-type: none"> - N. N'effectuez pas de démarrage spécial. Effectuez un démarrage à froid ou à chaud, tel que l'indique le paramètre coldstart. <p>La valeur par défaut est N.</p> <p>Remarque: vous devez indiquer le chemin d'accès complet dans les paramètres config, cs et license uniquement si le fichier ne se trouve <i>pas</i> dans le répertoire d'installation. Placez les chemins d'accès et les noms de fichier qui contiennent des espaces entre guillemets.</p>
-SvcPort -vp	service_port	Facultatif. Port sur lequel le service de journalisation surveille les commandes du gestionnaire de service.

DisplayAllLogger

Affiche tous les messages qui peuvent être produits par les autres commandes d'affichage du service de journalisation PowerExchange, triés par commande.

La commande infacmd pwx DisplayAllLogger affiche la sortie consolidée pour les commandes suivantes :

- DisplayCPULogger
- DisplayEventsLogger
- DisplayMemoryLogger
- DisplayRecordsLogger
- DisplayStatusLogger

La commande infacmd pwx DisplayAllLogger utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd pwx DisplayAllLogger :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de journalisation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel la commande infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.
-OSUser -oun	OS_user_name	<p>Obligatoire si vous activez la sécurité du système d'exploitation. Nom d'utilisateur pour le système d'exploitation.</p> <p>Activez la sécurité du système d'exploitation comme suit :</p> <ul style="list-style-type: none"> - Pour imposer aux utilisateurs de fournir dans la commande un identifiant et un mot de passe utilisateur du système d'exploitation valides, spécifiez 1 ou 2 dans le premier paramètre de l'instruction SECURITY dans le fichier de configuration DBMOVER sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange utilise les fonctions du système d'exploitation du système cible pour authentifier l'identifiant et le mot de passe utilisateur pour l'utilisation du programme infacmd pwx. - Pour autoriser les utilisateurs à exécuter des commandes infacmd pwx, spécifiez 2 dans le premier paramètre de l'instruction SECURITY et définissez les instructions AUTHGROUP et USER dans le fichier sign-on PowerExchange sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange vérifie le fichier Sign-On pour déterminer si l'identifiant utilisateur fourni est autorisé à exécuter des commandes dans le programme infacmd pwx.

Option	Argument	Description
-OSPassword -oup	OS_password	Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe crypté. Mot de passe pour le système d'exploitation. Vous pouvez définir un mot de passe en texte clair avec l'option -p ou avec la variable d'environnement INFA_DEFAULT_PWX_OSPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -p est prioritaire.
-OSEPassword -ouep	OS_epassword	Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe en texte clair. Mot de passe crypté pour le système d'exploitation. Vous pouvez définir un mot de passe crypté avec l'option -e ou la variable d'environnement INFA_DEFAULT_PWX_OSEPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -e est prioritaire.

DisplayCPULogger

Affiche la durée CPU, en microsecondes, utilisée par le service de journalisation PowerExchange pour chaque phase de traitement pendant le cycle de journalisation actuel. Inclut également la durée CPU totale de tous les traitements du service de journalisation.

Par exemple, la commande `infacmd pwx DisplayCPULogger` peut rapporter le temps CPU passé par le service de journalisation pour effectuer les actions suivantes :

- Lire les données source
- Écrire les données dans les fichiers journaux du service de journalisation
- Effectuer les basculements de fichier
- Effectuer d'autres traitements, tels que des commandes d'initialisation et de traitement

La commande `infacmd pwx DisplayCPULogger` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd pwx DisplayCPULogger :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de journalisation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel la commande infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.

Option	Argument	Description
-OSUser -oun	OS_user_name	<p>Obligatoire si vous activez la sécurité du système d'exploitation. Nom d'utilisateur pour le système d'exploitation.</p> <p>Activez la sécurité du système d'exploitation comme suit :</p> <ul style="list-style-type: none"> - Pour imposer aux utilisateurs de fournir dans la commande un identifiant et un mot de passe utilisateur du système d'exploitation valides, spécifiez 1 ou 2 dans le premier paramètre de l'instruction SECURITY dans le fichier de configuration DBMOVER sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange utilise les fonctions du système d'exploitation du système cible pour authentifier l'identifiant et le mot de passe utilisateur pour l'utilisation du programme infacmd pwx. - Pour autoriser les utilisateurs à exécuter des commandes infacmd pwx, spécifiez 2 dans le premier paramètre de l'instruction SECURITY et définissez les instructions AUTHGROUP et USER dans le fichier sign-on PowerExchange sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange vérifie le fichier Sign-On pour déterminer si l'identifiant utilisateur fourni est autorisé à exécuter des commandes dans le programme infacmd pwx.
-OSPassword -oup	OS_password	<p>Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe crypté. Mot de passe pour le système d'exploitation.</p> <p>Vous pouvez définir un mot de passe en texte clair avec l'option -p ou avec la variable d'environnement INFA_DEFAULT_PWX_OSPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -p est prioritaire.</p>
-OSEPassword -oue	OS_epassword	<p>Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe en texte clair. Mot de passe crypté pour le système d'exploitation.</p> <p>Vous pouvez définir un mot de passe crypté avec l'option -e ou la variable d'environnement INFA_DEFAULT_PWX_OSEPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -e est prioritaire.</p>

DisplayEventsLogger

Affiche les événements utilisés par les tâches Controller, Command Handler et Writer du service de journalisation PowerExchange. Indique également si le programme d'écriture est en cours de traitement des données ou en état de veille, en attente d'un événement ou du dépassement du délai.

La commande infacmd pwx DisplayEventsLogger utilise la syntaxe suivante :

```
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]

```

Le tableau suivant décrit les options et arguments d'infacmd pwx DisplayEventsLogger :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de journalisation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel la commande infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.
-OSUser -oun	OS_user_name	<p>Obligatoire si vous activez la sécurité du système d'exploitation. Nom d'utilisateur pour le système d'exploitation.</p> <p>Activez la sécurité du système d'exploitation comme suit :</p> <ul style="list-style-type: none"> - Pour imposer aux utilisateurs de fournir dans la commande un identifiant et un mot de passe utilisateur du système d'exploitation valides, spécifiez 1 ou 2 dans le premier paramètre de l'instruction SECURITY dans le fichier de configuration DBMOVER sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange utilise les fonctions du système d'exploitation du système cible pour authentifier l'identifiant et le mot de passe utilisateur pour l'utilisation du programme infacmd pwx. - Pour autoriser les utilisateurs à exécuter des commandes infacmd pwx, spécifiez 2 dans le premier paramètre de l'instruction SECURITY et définissez les instructions AUTHGROUP et USER dans le fichier sign-on PowerExchange sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange vérifie le fichier Sign-On pour déterminer si l'identifiant utilisateur fourni est autorisé à exécuter des commandes dans le programme infacmd pwx.

Option	Argument	Description
-OSPassword -oup	OS_password	Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe crypté. Mot de passe pour le système d'exploitation. Vous pouvez définir un mot de passe en texte clair avec l'option -p ou avec la variable d'environnement INFA_DEFAULT_PWX_OSPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -p est prioritaire.
-OSEPassword -ouep	OS_epassword	Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe en texte clair. Mot de passe crypté pour le système d'exploitation. Vous pouvez définir un mot de passe crypté avec l'option -e ou la variable d'environnement INFA_DEFAULT_PWX_OSEPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -e est prioritaire.

DisplayMemoryLogger

Affiche l'utilisation de la mémoire, en octets, pour chaque tâche et sous-tâche du service de journalisation PowerExchange, avec les totaux pour le processus du service de journalisation dans son ensemble.

PowerExchange fournit l'utilisation de la mémoire pour les catégories suivantes :

- Application. Mémoire demandée par l'application du service de journalisation pour son utilisation propre.
- Total. Mémoire totale utilisée pour l'application du service de journalisation et pour la surcharge due aux en-têtes associés. Cette valeur fluctue en fonction de l'allocation et de la libération de mémoire par PowerExchange lors du traitement du service de journalisation.
- Maximum. La quantité de mémoire la plus importante enregistrée pour la catégorie Total jusqu'au moment où cette commande s'exécute.

La commande infacmd pwx DisplayMemoryLogger utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd pwx DisplayMemoryLogger :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de journalisation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel la commande infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.
-OSUser -oun	OS_user_name	<p>Obligatoire si vous activez la sécurité du système d'exploitation. Nom d'utilisateur pour le système d'exploitation.</p> <p>Activez la sécurité du système d'exploitation comme suit :</p> <ul style="list-style-type: none"> - Pour imposer aux utilisateurs de fournir dans la commande un identifiant et un mot de passe utilisateur du système d'exploitation valides, spécifiez 1 ou 2 dans le premier paramètre de l'instruction SECURITY dans le fichier de configuration DBMOVER sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange utilise les fonctions du système d'exploitation du système cible pour authentifier l'identifiant et le mot de passe utilisateur pour l'utilisation du programme infacmd pwx. - Pour autoriser les utilisateurs à exécuter des commandes infacmd pwx, spécifiez 2 dans le premier paramètre de l'instruction SECURITY et définissez les instructions AUTHGROUP et USER dans le fichier sign-on PowerExchange sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange vérifie le fichier Sign-On pour déterminer si l'identifiant utilisateur fourni est autorisé à exécuter des commandes dans le programme infacmd pwx.
-OSPassword -oup	OS_password	<p>Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe crypté. Mot de passe pour le système d'exploitation.</p> <p>Vous pouvez définir un mot de passe en texte clair avec l'option -p ou avec la variable d'environnement INFA_DEFAULT_PWX_OSPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -p est prioritaire.</p>
-OSEPassword -ouep	OS_epassword	<p>Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe en texte clair. Mot de passe crypté pour le système d'exploitation.</p> <p>Vous pouvez définir un mot de passe crypté avec l'option -e ou la variable d'environnement INFA_DEFAULT_PWX_OSEPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -e est prioritaire.</p>

DisplayRecordsLogger

Affiche le nombre d'enregistrements de modifications traités par le service de journalisation PowerExchange pendant le cycle de traitement actuel. Si le service de journalisation n'a pas reçu de modifications dans le

cycle actuel, affiche le nombre d'enregistrements de modifications pour l'ensemble des fichiers journaux actuels du service de journalisation.

La commande `infacmd pwx DisplayRecordsLogger` affiche le nombre d'enregistrements pour chaque type d'enregistrement de modification traité et pour le nombre total d'enregistrements traités. Les types d'enregistrement de modification comprennent Delete, Insert, Update et Commit.

Selon que la commande affiche le compteur du cycle actuel ou des fichiers journaux actuels, la sortie comprendra tout ou partie des types d'informations suivants :

- **Cycle.** Le nombre d'enregistrements de modifications pour le cycle de traitement actuel du service de journalisation. Le service de journalisation réinitialise ces compteurs à zéro à l'expiration de l'intervalle d'attente spécifié dans le paramètre `NO_DATA_WAIT2` du fichier `pxxccl.cfg` et qu'aucune modification de données n'a été reçue.
- **File.** Nombre d'enregistrements de modifications de l'ensemble actuel des fichiers journaux PowerExchange. Le service de journalisation réinitialise ces compteurs à zéro quand un basculement de fichier se produit.
- **Total.** Nombre d'enregistrements de modifications que le service de journalisation a reçu depuis qu'il a démarré. PowerExchange ne réinitialise pas ces compteurs à zéro.

La commande `infacmd pwx DisplayRecordsLogger` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd pwx DisplayRecordsLogger :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de journalisation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel la commande infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.
-OSUser -oun	OS_user_name	<p>Obligatoire si vous activez la sécurité du système d'exploitation. Nom d'utilisateur pour le système d'exploitation.</p> <p>Activez la sécurité du système d'exploitation comme suit :</p> <ul style="list-style-type: none"> - Pour imposer aux utilisateurs de fournir dans la commande un identifiant et un mot de passe utilisateur du système d'exploitation valides, spécifiez 1 ou 2 dans le premier paramètre de l'instruction SECURITY dans le fichier de configuration DBMOVER sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange utilise les fonctions du système d'exploitation du système cible pour authentifier l'identifiant et le mot de passe utilisateur pour l'utilisation du programme infacmd pwx. - Pour autoriser les utilisateurs à exécuter des commandes infacmd pwx, spécifiez 2 dans le premier paramètre de l'instruction SECURITY et définissez les instructions AUTHGROUP et USER dans le fichier sign-on PowerExchange sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange vérifie le fichier Sign-On pour déterminer si l'identifiant utilisateur fourni est autorisé à exécuter des commandes dans le programme infacmd pwx.
-OSPassword -oup	OS_password	<p>Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe crypté. Mot de passe pour le système d'exploitation.</p> <p>Vous pouvez définir un mot de passe en texte clair avec l'option -p ou avec la variable d'environnement INFA_DEFAULT_PWX_OSPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -p est prioritaire.</p>
-OSEPassword -ouep	OS_epassword	<p>Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe en texte clair. Mot de passe crypté pour le système d'exploitation.</p> <p>Vous pouvez définir un mot de passe crypté avec l'option -e ou la variable d'environnement INFA_DEFAULT_PWX_OSEPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -e est prioritaire.</p>

displayStatsListener

Affiche les statistiques de surveillance d'un écouteur PowerExchange sous Linux, UNIX ou Windows géré par le service d'écoute PowerExchange. Affiche également les statistiques pour les tâches clientes et les connexions source ou cible qui sont associées à l'écouteur.

La commande peut imprimer les types suivants de statistiques, en fonction de l'option -type que vous spécifiez :

- Statistiques résumées de l'écouteur PowerExchange concernant l'utilisation de la mémoire, le temps de traitement du processeur et l'activité pour le compte des demandes clientes. Ces statistiques incluent le nombre de tâches clientes, de connexions, de messages envoyés et reçus, et d'octets de données envoyés et reçus.
- Volumes de messages et de données que les tâches clientes ont envoyés et reçus pour les demandes clientes, par ID de tâche et méthode d'accès. Les volumes de message et de données correspondent à des totaux au moment de la génération des statistiques.
- Informations sur les tâches actives qui sont exécutées sous l'écouteur pour exécuter les demandes clientes. Ces statistiques incluent l'heure de début de la tâche, le temps de traitement du processeur, la méthode d'accès, le mode lecture ou écriture et les ID de processus et de session associés. Comprend également le numéro de port et l'adresse IP du client qui a émis la demande à destination de l'écouteur PowerExchange.

Important: Pour que PowerExchange puisse collecter les statistiques de surveillance de l'écouteur PowerExchange, vous devez spécifier le paramètre MONITOR dans l'instruction STATS du fichier de configuration DBMOVER dans lequel l'écouteur est exécuté.

La commande infacmd pwx displayStatsListener utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd pwx displayStatsListener` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'écoute.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.

Option	Argument	Description
-OSUser -oun	OS_user_name	<p>Obligatoire si vous activez la sécurité du système d'exploitation. Nom d'utilisateur pour le système d'exploitation.</p> <p>Activez la sécurité du système d'exploitation comme suit :</p> <ul style="list-style-type: none"> - Pour imposer aux utilisateurs de fournir dans la commande un identifiant et un mot de passe utilisateur du système d'exploitation valides, spécifiez 1 ou 2 dans le premier paramètre de l'instruction SECURITY dans le fichier de configuration DBMOVER sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange utilise les fonctions du système d'exploitation du système cible pour authentifier l'identifiant et le mot de passe utilisateur pour l'utilisation du programme infacmd pwx. - Pour autoriser les utilisateurs à exécuter des commandes infacmd pwx, spécifiez 2 dans le premier paramètre de l'instruction SECURITY et définissez les instructions AUTHGROUP et USER dans le fichier sign-on PowerExchange sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange vérifie le fichier Sign-On pour déterminer si l'identifiant utilisateur fourni est autorisé à exécuter des commandes dans le programme infacmd pwx.
-OSPassword -oup	OS_password	<p>Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe crypté. Mot de passe pour le système d'exploitation.</p> <p>Vous pouvez définir un mot de passe en texte clair avec l'option -p ou avec la variable d'environnement INFA_DEFAULT_PWX_OSPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -p est prioritaire.</p>

Option	Argument	Description
-OSEPassword -ouep	OS_epassword	Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe en texte clair. Mot de passe crypté pour le système d'exploitation. Vous pouvez définir un mot de passe crypté avec l'option -e ou la variable d'environnement INFA_DEFAULT_PWX_OSEPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -e est prioritaire.
-type -tp	report_type	Facultatif. Type de statistiques de surveillance à signaler pour l'écouteur PowerExchange et ses tâches et connexions clientes. La valeur du paramètre report_type doit être l'une des suivantes : <ul style="list-style-type: none"> - listener. Pour un écouteur PowerExchange spécifique, signale l'utilisation de la mémoire, le temps de traitement du processeur, le nombre total de tâches clientes, les tâches actives, les tâches à limite supérieure, le nombre maximal de tâches autorisées, le nombre total de tentatives de connexion, les connexions acceptées, les connexions actives, le nombre de messages envoyés et reçus, et les octets de données envoyés et reçus. - accessmethods. Pour chaque méthode d'accès de chaque tâche active, signale le nombre de lignes lues et écrites, les octets de données lus et écrits, le nom du fichier source ou cible ou le nom du fichier de carte de données, selon la méthode d'accès, et le temps de traitement du processeur. - clients. Pour chaque tâche active, signale l'ID de tâche, le statut, la méthode d'accès, le mode lecture ou écriture, les ID de processus et de session, le cas échéant, le temps de traitement du processeur et la date et l'heure de début. Signale également le numéro de port et l'adresse IP du client qui a émis la demande pour laquelle la tâche a été créée. Si le client est PowerCenter, signale l'ID de session PowerCenter et le nom de l'application pour CDC. La valeur par défaut est l'écouteur. Remarque: Dans ces rapports, une méthode d'accès peut être un type de source comme NRDB. Une tâche cliente peut être associée à plusieurs méthodes d'accès : une pour lire les données source et une autre pour le mappage des données non relationnelles sur un format relationnel.

DisplayStatusLogger

Affiche le statut de la sous-tâche du programme d'écriture pour un service de journalisation PowerExchange.

Par exemple, la commande `infacmd pwx DisplayStatusLogger` peut signaler quand le programme d'écriture a terminé les actions suivantes :

- Initialise
- Lit ou attend les données source
- Enregistre les données source dans un fichier journal du service de journalisation
- Enregistre les enregistrements CDCT lors du basculement d'un fichier

- Supprime les enregistrements CDCT obsolètes
- Arrête

La commande `infacmd pwx DisplayStatusLogger` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de `infacmd pwx DisplayStatusLogger` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de journalisation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel la commande infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.
-OSUser -oun	OS_user_name	Obligatoire si vous activez la sécurité du système d'exploitation. Nom d'utilisateur pour le système d'exploitation. Activez la sécurité du système d'exploitation comme suit : <ul style="list-style-type: none"> - Pour imposer aux utilisateurs de fournir dans la commande un identifiant et un mot de passe utilisateur du système d'exploitation valides, spécifiez 1 ou 2 dans le premier paramètre de l'instruction SECURITY dans le fichier de configuration DBMOVER sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange utilise les fonctions du système d'exploitation du système cible pour authentifier l'identifiant et le mot de passe utilisateur pour l'utilisation du programme infacmd pwx. - Pour autoriser les utilisateurs à exécuter des commandes infacmd pwx, spécifiez 2 dans le premier paramètre de l'instruction SECURITY et définissez les instructions AUTHGROUP et USER dans le fichier sign-on PowerExchange sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange vérifie le fichier Sign-On pour déterminer si l'identifiant utilisateur fourni est autorisé à exécuter des commandes dans le programme infacmd pwx.

Option	Argument	Description
-OSPassword -oup	OS_password	Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe crypté. Mot de passe pour le système d'exploitation. Vous pouvez définir un mot de passe en texte clair avec l'option -p ou avec la variable d'environnement INFA_DEFAULT_PWX_OSPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -p est prioritaire.
-OSEPassword -ouep	OS_epassword	Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe en texte clair. Mot de passe crypté pour le système d'exploitation. Vous pouvez définir un mot de passe crypté avec l'option -e ou la variable d'environnement INFA_DEFAULT_PWX_OSEPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -e est prioritaire.

FileSwitchLogger

Ferme les fichiers journaux ouverts du service de journalisation PowerExchange et passe à un nouvel ensemble de fichiers journaux. Si les fichiers journaux ouverts ne contiennent pas de données, le basculement de fichier ne se produit pas.

Remarque: Si vous utilisez le mode d'extraction en continu, vous n'avez généralement pas besoin d'effectuer les basculements de fichier manuellement.

La commande `infacmd pwx FileSwitchLogger` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd pwx FileSwitchLogger :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de journalisation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel la commande infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.

Option	Argument	Description
-OSUser -oun	OS_user_name	<p>Obligatoire si vous activez la sécurité du système d'exploitation. Nom d'utilisateur pour le système d'exploitation.</p> <p>Activez la sécurité du système d'exploitation comme suit :</p> <ul style="list-style-type: none"> - Pour imposer aux utilisateurs de fournir dans la commande un identifiant et un mot de passe utilisateur du système d'exploitation valides, spécifiez 1 ou 2 dans le premier paramètre de l'instruction SECURITY dans le fichier de configuration DBMOVER sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange utilise les fonctions du système d'exploitation du système cible pour authentifier l'identifiant et le mot de passe utilisateur pour l'utilisation du programme infacmd pwx. - Pour autoriser les utilisateurs à exécuter des commandes infacmd pwx, spécifiez 2 dans le premier paramètre de l'instruction SECURITY et définissez les instructions AUTHGROUP et USER dans le fichier sign-on PowerExchange sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange vérifie le fichier Sign-On pour déterminer si l'identifiant utilisateur fourni est autorisé à exécuter des commandes dans le programme infacmd pwx.
-OSPassword -oup	OS_password	<p>Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe crypté. Mot de passe pour le système d'exploitation.</p> <p>Vous pouvez définir un mot de passe en texte clair avec l'option -p ou avec la variable d'environnement INFA_DEFAULT_PWX_OSPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -p est prioritaire.</p>
-OSEPassword -ouep	OS_epassword	<p>Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe en texte clair. Mot de passe crypté pour le système d'exploitation.</p> <p>Vous pouvez définir un mot de passe crypté avec l'option -e ou la variable d'environnement INFA_DEFAULT_PWX_OSEPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -e est prioritaire.</p>

ListTaskListener

Affiche les informations concernant chaque tâche active de l'Ecouteur PowerExchange, y compris l'adresse TCP/IP, le numéro de port, le nom de l'application, le type d'accès et le statut.

La commande infacmd pwx ListTaskListener utilise la syntaxe suivante :

```
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]

```

Le tableau suivant décrit les options et arguments d'infacmd pwx ListTaskListener :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'écoute.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel la commande infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.
-OSUser -oun	OS_user_name	<p>Obligatoire si vous activez la sécurité du système d'exploitation. Nom d'utilisateur pour le système d'exploitation.</p> <p>Activez la sécurité du système d'exploitation comme suit :</p> <ul style="list-style-type: none"> - Pour imposer aux utilisateurs de fournir dans la commande un identifiant et un mot de passe utilisateur du système d'exploitation valides, spécifiez 1 ou 2 dans le premier paramètre de l'instruction SECURITY dans le fichier de configuration DBMOVER sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange utilise les fonctions du système d'exploitation du système cible pour authentifier l'identifiant et le mot de passe utilisateur pour l'utilisation du programme infacmd pwx. - Pour autoriser les utilisateurs à exécuter des commandes infacmd pwx, spécifiez 2 dans le premier paramètre de l'instruction SECURITY et définissez les instructions AUTHGROUP et USER dans le fichier sign-on PowerExchange sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange vérifie le fichier Sign-On pour déterminer si l'identifiant utilisateur fourni est autorisé à exécuter des commandes dans le programme infacmd pwx.

Option	Argument	Description
-OSPassword -oup	OS_password	Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe crypté. Mot de passe pour le système d'exploitation. Vous pouvez définir un mot de passe en texte clair avec l'option -p ou avec la variable d'environnement INFA_DEFAULT_PWX_OSPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -p est prioritaire.
-OSEPassword -oue	OS_epassword	Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe en texte clair. Mot de passe crypté pour le système d'exploitation. Vous pouvez définir un mot de passe crypté avec l'option -e ou la variable d'environnement INFA_DEFAULT_PWX_OSEPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -e est prioritaire.

ShutDownLogger

Interrompt le service de journalisation PowerExchange de façon contrôlée. La commande ferme les fichiers journaux du service de journalisation et écrit ensuite la dernière position de redémarrage dans les fichiers CDCT.

Utilisez cette commande pour arrêter un service de journalisation PowerExchange qui s'exécute en mode continu.

Lors du processus de fermeture, le service de journalisation effectue les actions suivantes :

- Ferme les fichiers journaux ouverts
- Écrit les informations mises à jour dans le fichier CDCT, y compris les jetons de redémarrage et de séquence
- Ferme CAPI
- Interrompt le programme d'écriture et les sous-tâches du gestionnaire de commande
- Termine le programme pwxcc
- Signale les utilisations CPU

La commande infacmd pwx ShutDownLogger utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd pwx ShutDownLogger :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de journalisation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel la commande infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.
-OSUser -oun	OS_user_name	<p>Obligatoire si vous activez la sécurité du système d'exploitation. Nom d'utilisateur pour le système d'exploitation.</p> <p>Activez la sécurité du système d'exploitation comme suit :</p> <ul style="list-style-type: none"> - Pour imposer aux utilisateurs de fournir dans la commande un identifiant et un mot de passe utilisateur du système d'exploitation valides, spécifiez 1 ou 2 dans le premier paramètre de l'instruction SECURITY dans le fichier de configuration DBMOVER sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange utilise les fonctions du système d'exploitation du système cible pour authentifier l'identifiant et le mot de passe utilisateur pour l'utilisation du programme infacmd pwx. - Pour autoriser les utilisateurs à exécuter des commandes infacmd pwx, spécifiez 2 dans le premier paramètre de l'instruction SECURITY et définissez les instructions AUTHGROUP et USER dans le fichier sign-on PowerExchange sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange vérifie le fichier Sign-On pour déterminer si l'identifiant utilisateur fourni est autorisé à exécuter des commandes dans le programme infacmd pwx.

Option	Argument	Description
-OSPassword -oup	OS_password	Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe crypté. Mot de passe pour le système d'exploitation. Vous pouvez définir un mot de passe en texte clair avec l'option -p ou avec la variable d'environnement INFA_DEFAULT_PWX_OSPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -p est prioritaire.
-OSEPassword -ouep	OS_epassword	Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe en texte clair. Mot de passe crypté pour le système d'exploitation. Vous pouvez définir un mot de passe crypté avec l'option -e ou la variable d'environnement INFA_DEFAULT_PWX_OSEPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -e est prioritaire.

StopTaskListener

Arrête une tâche de l'Ecouteur PowerExchange correspondant au nom d'application ou à l'identifiant de tâche que vous indiquez. Lors de la modification de l'extraction de données, infacmd pwx StopTaskListener attend, pour arrêter la tâche, de rencontrer la terminaison UOW ou d'atteindre le seuil de validation.

La commande infacmd pwx StopTaskListener utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd pwx StopTaskListener :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'écoute.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port des nœuds de passerelle du domaine.

Option	Argument	Description
-OSUser -oun	OS_user_name	<p>Obligatoire si vous activez la sécurité du système d'exploitation. Nom d'utilisateur pour le système d'exploitation.</p> <p>Activez la sécurité du système d'exploitation comme suit :</p> <ul style="list-style-type: none"> - Pour imposer aux utilisateurs de fournir dans la commande un identifiant et un mot de passe utilisateur du système d'exploitation valides, spécifiez 1 ou 2 dans le premier paramètre de l'instruction SECURITY dans le fichier de configuration DBMOVER sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange utilise les fonctions du système d'exploitation du système cible pour authentifier l'identifiant et le mot de passe utilisateur pour l'utilisation du programme infacmd pwx. - Pour autoriser les utilisateurs à exécuter des commandes infacmd pwx, spécifiez 2 dans le premier paramètre de l'instruction SECURITY et définissez les instructions AUTHGROUP et USER dans le fichier sign-on PowerExchange sur chaque système Linux, UNIX ou Windows ciblé par la commande. PowerExchange vérifie le fichier Sign-On pour déterminer si l'identifiant utilisateur fourni est autorisé à exécuter des commandes dans le programme infacmd pwx.
-OSPassword -oup	OS_password	<p>Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe crypté. Mot de passe pour le système d'exploitation.</p> <p>Vous pouvez définir un mot de passe en texte clair avec l'option -p ou avec la variable d'environnement INFA_DEFAULT_PWX_OSPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -p est prioritaire.</p>
-OSEPassword -ouep	OS_epassword	<p>Obligatoire si vous spécifiez un nom d'utilisateur mais pas de mot de passe en texte clair. Mot de passe crypté pour le système d'exploitation.</p> <p>Vous pouvez définir un mot de passe crypté avec l'option -e ou la variable d'environnement INFA_DEFAULT_PWX_OSEPASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -e est prioritaire.</p>
-applicationid -a	appname	<p>Requis si vous ne spécifiez pas -taskid.</p> <p>Nom de l'application. Nom du processus d'extraction active à arrêter. Le message PWX-00712 de la sortie de commande infacmd pwx listtaskListener affiche ce nom.</p>
-taskid -t	taskid	<p>Requis si vous ne spécifiez pas -application.</p> <p>ID de tâche du service d'écoute. Identificateur numérique de la tâche du service d'écoute à arrêter.</p> <p>Astuce: Pour déterminer le nom de la tâche active, exécutez la commande infacmd pwx listtaskListener. Dans la sortie de commande, la valeur du nom dans le message PWX-00712 comporte l'identifiant de tâche.</p>

UpgradeModels

Met à niveau les objets de données non relationnels PowerExchange 9.0.1. Vous devez mettre à niveau les objets de données avant de pouvoir les utiliser.

La commande affiche les résultats de la mise à niveau, triés par nom de connexion, puis par schéma et nom du mappage. Vous pouvez exécuter la commande UpgradeModels plusieurs fois si certains objets ne sont pas mis à niveau la première fois.

La commande vérifie que la carte de données est compatible avec les opérations non relationnelles qui ont été définies pour elle lors de l'importation de l'objet non relationnel. Si des différences existent, les opérations non relationnelles sont supprimées et recrées pour correspondre à la carte de données. Vous devez modifier tout mappage ou mapplet affecté pour utiliser les opérations non relationnelles qui ont été recrées.

La commande infacmd pwx UpgradeModels utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd pwx UpgradeModels :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-MrsServiceName -msn	mrs_service_name	Requis. Nom du service de référentiel modèle. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 230 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "
-ConnectionName -cn	connection_name	Requis. Nom de la connexion contenant les objets de données non relationnels à mettre à niveau. Pour spécifier toutes les connexions ou les connexions ayant le même modèle de début de nom, incluez le caractère générique astérisque (*) entre guillemets doubles, par exemple « * » ou ABC« * ».
-DataObjectSchemaName -ds	data_object_schema_name	Requis. Nom du schéma contenant les cartes de données des objets de données non relationnels à mettre à niveau. Pour spécifier tous les schémas ou les schémas ayant le même modèle de début de nom, incluez le caractère générique astérisque (*) entre guillemets doubles, par exemple « * » ou ABC« * ».
-DataObjectName -do	data_object_name	Requis. Nom de la carte de données de l'objet de données non relationnel à mettre à niveau. Pour spécifier toutes les cartes de données ou les cartes de données ayant le même modèle de début de nom, incluez le caractère générique astérisque (*) entre guillemets doubles, par exemple « * » ou ABC« * ».
-Preview -pr	aperçu	Requis. Spécifiez Y pour afficher un aperçu des résultats de la mise à niveau sans les valider ou N pour mettre à niveau les objets. Pour vous assurer que la commande s'exécutera correctement, exécutez la commande UpgradeModels en affectant la valeur Y à Preview avant de procéder à la mise à niveau effective.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Facultatif. Nom du service d'écoute. La première commande utilise le nom de connexion pour récupérer les cartes de données spécifiées. Si la tentative échoue, la commande utilise le nom du service d'écoute pour récupérer les cartes de données. Le nom n'est pas sensible à la casse. Le nom ne peut pas dépasser 128 caractères ou contenir des retours chariot, des tabulations, des espaces ou les caractères suivants : / * ? < > "

UpdateListenerService

Met à jour les propriétés d'un service d'écoute PowerExchange.

La commande infacmd pwx UpdateListenerService utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande `infacmd pwx UpdateListenerService` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'écoute.
-LicenseName -ln	license_name	Facultatif. Licence à attribuer au service. Si elle n'est pas déjà fournie, obligatoire pour pouvoir activer le service.
-NodeName -nn	node_name	Requis. Nom du nœud sur lequel vous souhaitez que le service d'écoute s'exécute.
-BackupNode -bn	backup_node	Facultatif. Si l'environnement PowerCenter est configuré pour une haute disponibilité, cette option spécifie le nom du nœud de sauvegarde.

Option	Argument	Description
-StartParameters -sp	start_parameters	<p>Facultatif. Paramètres à inclure lorsque vous démarrez le service d'écoute. Séparez les paramètres par un espace.</p> <p>Vous pouvez inclure les paramètres suivants :</p> <ul style="list-style-type: none"> - <i>node_name</i> Nom du nœud qui identifie le service d'écoute. Ce nom doit correspondre à celui de l'instruction LISTENER dans le fichier de configuration DBMOVER. - <i>config=directory</i> Spécifie le chemin d'accès complet et le nom de fichier de tout fichier de configuration à préférer au fichier dbmover.cfg par défaut. Cet autre fichier de configuration est prioritaire sur tout fichier de configuration spécifié dans la variable d'environnement PWX_CONFIG. - <i>license=directory/license_key_file</i> Spécifie le chemin d'accès complet et le nom de tout fichier de clé de licence à préférer au fichier license.key par défaut. Le nom ou le chemin d'accès du fichier de clé de licence de substitution doit différer de celui du fichier par défaut. Cet autre fichier de clé de licence est prioritaire sur tout fichier de clé de licence spécifié dans la variable d'environnement PWX_LICENSE. <p>Remarque: Dans les paramètres config et license, vous devez indiquer le chemin d'accès complet uniquement si le fichier ne se trouve <i>pas</i> dans le répertoire d'installation. Placez les chemins d'accès et les noms de fichier qui contiennent des espaces entre guillemets.</p>
-SvcPort -sp	service_port	<p>Facultatif. Port sur lequel le service d'écoute surveille les commandes émises par le gestionnaire de service.</p>

UpdateLoggerService

Met à jour les propriétés d'un service de journalisation PowerExchange.

La commande infacmd pwx UpdateLoggerService utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande `infacmd pwx UpdateLoggerService` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de journalisation.
-NodeName -nn	node_name	Requis. Nom du nœud sur lequel vous souhaitez que le service de journalisation s'exécute.
-LicenseName -ln	license_name	Licence à attribuer au service. Si elle n'est pas déjà fournie, obligatoire pour pouvoir activer le service.
-BackupNode -bn	backup_node	Facultatif. Si l'environnement PowerCenter est configuré pour une haute disponibilité, cette option spécifie le nom du nœud de sauvegarde.

Option	Argument	Description
-StartParameters -sp	start_parameters	<p>Facultatif. Paramètres à inclure lorsque vous démarrez le service de journalisation. Séparez les paramètres par un espace.</p> <p>Vous pouvez inclure les paramètres suivants :</p> <ul style="list-style-type: none"> - coldstart={Y N} Indique si le service de journalisation doit être démarré à froid ou à chaud. Entrez Y pour démarrer le service de journalisation à froid. Si le fichier CDCT contient des enregistrements de journaux, le service de journalisation les supprime. Entrez N pour démarrer le service de journalisation à chaud à partir du point de redémarrage indiqué dans le fichier CDCT. La valeur par défaut est N. - config=directory/pwx_config_file Spécifie le chemin d'accès complet et le nom de fichier de tout fichier de configuration à préférer au fichier dbmover.cfg par défaut. Cet autre fichier de configuration est prioritaire sur tout fichier de configuration spécifié dans la variable d'environnement PWX_CONFIG. - cs=directory/pwxlogger_config_file Spécifie le chemin d'accès et le nom du fichier de configuration du service de journalisation. Vous pouvez également utiliser le paramètre cs pour indiquer un fichier de configuration du service de journalisation qui remplace le fichier pwxcl.cfg par défaut. Le nom ou le chemin d'accès du fichier de substitution doit différer de celui du fichier par défaut. - encryptpwd=encrypted_password Mot de passe au format crypté qui permet d'activer le cryptage des fichiers journaux du service de journalisation PowerExchange. Avec ce mot de passe, le service de journalisation PowerExchange peut générer une clé de cryptage unique pour chaque fichier journal du service. Le mot de passe est stocké dans le fichier CDCT au format crypté. Pour des raisons de sécurité, le mot de passe n'est pas stocké dans des fichiers de sauvegarde CDCT et n'est pas affiché dans les rapports CDCT que vous pouvez générer avec l'utilitaire PWXUCDCT de PowerExchange. Si vous définissez ce paramètre, vous devez également définir coldstart sur Y. Si vous définissez ce paramètre, mais définissez également le paramètre ENCRYPTPWD dans le fichier de configuration du service de journalisation PowerExchange (pwxcl.cfg), le paramètre défini dans le fichier de configuration est prioritaire. Si vous définissez ce paramètre ainsi que le paramètre ENCRYPTPWD dans le fichier de configuration du service de journalisation PowerExchange, une erreur se produit. Vous pouvez définir l'algorithme AES à utiliser pour le cryptage du fichier journal dans le paramètre ENCRYPTOPT du fichier pwxcl.cfg. La valeur par défaut est AES128. Astuce: pour optimiser la sécurité, Informatica recommande de spécifier le mot de passe de cryptage lors du démarrage à froid du service de journalisation

Option	Argument	Description
		<p>PowerExchange, plutôt que de le spécifier dans le fichier de configuration pwxcl.cfg. Cette pratique peut réduire les risques d'accès malveillant au mot de passe de cryptage pour les raisons suivantes : 1) Le mot de passe de cryptage n'est pas stocké dans le fichier pwxcl.cfg. 2) Vous pouvez supprimer le mot de passe de la ligne de commande après le démarrage à froid. Si vous spécifiez le cryptage de mot de passe pour un démarrage à froid et que vous devez restaurer le fichier CDCT par la suite, vous devez entrer le même mot de passe de cryptage dans la commande RESTORE_CDCT de l'utilitaire PWXUCDCT.</p> <p>Pour <i>ne pas</i> crypter les fichiers journaux du service de journalisation PowerExchange, n'entrez pas de mot de passe de cryptage.</p> <ul style="list-style-type: none"> - <code>license=directory/license_key_file</code> Spécifie le chemin d'accès complet et le nom de tout fichier de clé de licence à préférer au fichier license.key par défaut. Le nom ou le chemin d'accès du fichier de clé de licence de substitution doit différer de celui du fichier par défaut. Cet autre fichier de clé de licence est prioritaire sur tout fichier de clé de licence spécifié dans la variable d'environnement PWX_LICENSE. - <code>specialstart={Y N}</code> Indique si vous effectuez un démarrage spécial pour le service de journalisation PowerExchange. Un démarrage spécial commence par un processus de capture de PowerExchange à partir du point du flux de modifications que vous spécifiez dans le fichier pwxcl.cfg. Ce point de démarrage remplace le point de redémarrage défini dans le fichier CDCT pour l'exécution du service de journalisation PowerExchange. Un démarrage spécial ne supprime aucun contenu du fichier CDCT. Utilisez ce paramètre pour ignorer les sections problématiques dans les journaux sources sans perdre les données capturées. Par exemple, utilisez le démarrage spécial dans les cas suivants : <ul style="list-style-type: none"> - Vous ne souhaitez pas que le service de journalisation PowerExchange capture la mise à niveau d'un catalogue Oracle. Dans ce cas, arrêtez le service de journalisation PowerExchange avant la mise à niveau. Une fois la mise à niveau terminée, générez une nouvelle séquence et des jetons de redémarrage pour le service de journalisation PowerExchange selon le SCN après la mise à niveau. Entrez la valeur de ces jetons dans les paramètres SEQUENCE_TOKEN et RESTART_TOKEN du fichier pwxcl.cfg, puis effectuez un démarrage spécial du service de journalisation PowerExchange. - Vous ne souhaitez pas que le service de journalisation PowerExchange traite à nouveau les journaux anciens et indisponibles provoqués par des unités de travail en cours non pertinentes pour CDC. Dans ce cas, arrêtez le service de journalisation PowerExchange. Modifiez la valeur RESTART_TOKEN de manière à refléter la valeur SCN du journal le plus récent disponible, puis effectuez un démarrage spécial. Si l'une des unités de travail en cours ayant démarré avant ce point de redémarrage est pertinente pour CDC, des données peuvent être perdues.

Option	Argument	Description
		<p>Valeurs valides :</p> <ul style="list-style-type: none"> - Y. Effectuez un démarrage spécial du service de journalisation PowerExchange depuis le point du flux de modifications défini dans les valeurs des paramètres SEQUENCE_TOKEN et RESTART_TOKEN dans le fichier de configuration pwxcl.cfg. Vous devez spécifier des valeurs de jetons valides dans le fichier pwxcl.cfg. pour effectuer un démarrage spécial. Ces valeurs de jeton remplacent celles du fichier CDCT. Vérifiez que la valeur SEQUENCE_TOKEN dans le fichier pwxcl.cfg est supérieure ou égale à celle du jeton de la séquence actuelle dans le fichier CDCT. <p>Enfin, ne définissez pas le paramètre coldstart sur Y. Sinon, ce paramètre devient prioritaire.</p> <ul style="list-style-type: none"> - N. N'effectuez pas de démarrage spécial. Effectuez un démarrage à froid ou à chaud, tel que l'indique le paramètre coldstart. <p>La valeur par défaut est N.</p> <p>Remarque: Dans les paramètres config, cs et license, vous devez indiquer le chemin d'accès complet uniquement si le fichier ne se trouve <i>pas</i> dans le répertoire d'installation. Placez les chemins d'accès et les noms de fichier qui contiennent des espaces entre guillemets.</p>
-SvcPort -sp	service_port	Port sur lequel le service de journalisation surveille les commandes du gestionnaire de service.

CHAPITRE 30

Référence de commande infacmd roh

Ce chapitre comprend les rubriques suivantes :

- [listProcessProperties, 1052](#)
- [listReverseProxyServerOptions, 1054](#)
- [listServiceProcessOptions, 1055](#)
- [listServiceOptions, 1057](#)
- [updateReverseProxyServerOptions, 1058](#)
- [updateServiceProcessOptions, 1060](#)
- [updateServiceOptions, 1062](#)

listProcessProperties

Répertorie les propriétés du processus de Hub des opérations REST.

La syntaxe de la commande infacmd roh listProcessProperties est la suivante :

```
<-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]
```


Le tableau suivant décrit les options et les arguments de la commande `infacmd roh listProcessProperties` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user-name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	Domain gateway host:port	Obligatoire si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Entrez le nom d'hôte et le numéro de port correspondant au nœud de passerelle dans le domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

listReverseProxyServerOptions

Répertorie les propriétés du serveur proxy inverse.

La syntaxe de la commande infacmd roh listReverseProxyServerOptions est la suivante :

```
<-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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd roh listReverseProxyServerOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom de domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est Natif. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-NodeName -nn	Node_name	Obligatoire. Nœud sur lequel s'exécute le processus du service.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

listServiceProcessOptions

Répertorie les propriétés du processus de service Hub des opérations REST.

La syntaxe de la commande infacmd roh listServiceProcessOptions est la suivante :

```
<-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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd roh listServiceProcessOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom de domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est <code>Natif</code> . Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-NodeName -nn	Node_name	Obligatoire. Nœud sur lequel s'exécute le processus du service.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

listServiceOptions

Répertorie les propriétés du service Hub des opérations REST.

La syntaxe de la commande infacmd roh listServiceOptions est la suivante :

```
<-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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd roh listServiceOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom de domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est Natif. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

updateReverseProxyServerOptions

Met à jour les propriétés du serveur proxy inverse.

La syntaxe de la commande infacmd roh updateReverseProxyServerOptions est la suivante :

```
<-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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd roh updateReverseProxyServerOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom de domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est <code>Natif</code> . Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-NodeName -nn	Node_name	Obligatoire. Nœud sur lequel s'exécute le processus du service.

Option	Argument	Description
- ServiceProcessReverseProxyServerOptions -so	option_name=value ...	Facultatif. Propriétés du processus de service qui définissent le mode d'exécution du serveur proxy inverse.
-Options -o	option	Facultatif. Entrez chaque option de propriété personnalisée en la séparant de la suivante par un espace. Utilisez le préfixe <code>RPS:</code> avec la paire nom et valeur. Par exemple, <code>RPS:<custom_property>=<custom_value>.</code>
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option <code>-re</code> ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option <code>-re</code> est prioritaire.

updateServiceProcessOptions

Met à jour les propriétés du processus de service Hub des opérations REST dans un domaine.

La syntaxe de la commande `infacmd roh updateServiceProcessOptions` est la suivante :

```
<-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]
```


Le tableau suivant décrit les options et les arguments de la commande `infacmd roh updateServiceProcessOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom de domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est <code>Natif</code> . Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-NodeName -nn	Node_name	Requis. Nœud sur lequel s'exécute le processus du service.
-ServiceOptions -so	option_name=value ...	Facultatif. Propriétés de service qui définissent le mode d'exécution du service Hub des opérations REST.
-Options -o	option	Facultatif. Entrez chaque option de propriété personnalisée en la séparant de la suivante par un espace. Utilisez le préfixe <code>ROH:</code> avec la paire nom et valeur. Par exemple, <code>ROH:<custom_property>=<custom_value></code> .

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

updateServiceOptions

Met à jour les propriétés du service Hub des opérations REST.

La commande infacmd roh updateServiceOptions utilise la syntaxe suivante :

```
<-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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd roh updateServiceOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom de domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est Natif. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-NodeName -nn	Node_name	Requis. Nom du nœud qui appartient à une grille dans laquelle le processus s'exécute.
-GridName -gn	grid_name	Requis. Nom de la grille.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Options -o	option	Facultatif. Entrez chaque option de propriété personnalisée en la séparant de la suivante par un espace. Utilisez le préfixe RPS: pour définir le serveur proxy inverse ou le préfixe ROH: pour définir la propriété personnalisée du Hub des opérations REST. Par exemple, RPS:<custom_property>=<custom_value>.

CHAPITRE 31

Référence de commande infacmd rms

Ce chapitre comprend les rubriques suivantes :

- [ListComputeNodeAttributes, 1064](#)
- [ListServiceOptions, 1066](#)
- [SetComputeNodeAttributes, 1067](#)
- [UpdateServiceOptions, 1069](#)

ListComputeNodeAttributes

Répertorie les attributs du nœud de calcul qui ont été remplacés pour le nœud spécifié ou pour tous les nœuds. Utilisez la commande infacmd rms SetComputeNodeAttributes pour remplacer les attributs de nœud de calcul.

Les valeurs par défaut des attributs sont le nombre réel de cœurs et la mémoire disponible sur la machine. Si la commande infacmd rms ListComputeNodeAttributes ne répertorie pas de valeur pour un attribut, le service du gestionnaire de ressource utilise les valeurs par défaut.

La commande infacmd rms ListComputeNodeAttributes utilise la syntaxe suivante :

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

Le tableau suivant décrit les options et les arguments de la commande `infacmd rms ListComputeNodeAttributes` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-NodeName -nn	node_name	Facultatif. Nom du nœud de calcul pour lequel vous voulez répertorier les attributs. Si vous omettez cette option, la commande répertorie tous les nœuds de calcul du domaine.
-ServiceName -sn	service_name	Facultatif. Entrez <code>Resource_Manager_Service</code> .

ListServiceOptions

Répertorie les propriétés du service du gestionnaire de ressource.

La commande infacmd rms ListServiceOptions utilise la syntaxe suivante\~:

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd rms ListServiceOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Facultatif. Entrez Resource_Manager_Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

SetComputeNodeAttributes

Remplace les attributs de nœud de calcul du nœud spécifié.

Les valeurs par défaut des attributs sont le nombre réel de cœurs et la mémoire disponible sur la machine. Pour réinitialiser une option sur sa valeur par défaut, spécifiez -1 comme valeur.

La commande infacmd rms SetComputeNodeAttributes utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd rms`
`SetComputeNodeAttributes` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-NodeName -nn	node_name	Requis. Nom du nœud de calcul pour lequel vous voulez définir des attributs.

Option	Argument	Description
-MaxCores -mc	max_number_of_cores_to_allocate	Facultatif. Nombre maximal de cœurs que le service du gestionnaire de ressource peut allouer aux tâches qui s'exécutent sur le nœud de calcul. Un nœud de calcul nécessite au moins cinq cœurs disponibles pour initialiser un conteneur de façon à démarrer un processus DTM. Si l'un des nœuds de calcul attribués à la grille a moins de cinq cœurs, ce nombre est utilisé comme nombre minimal de cœurs requis pour initialiser un conteneur. Par défaut, le nombre maximal de cœurs est le nombre réel de cœurs disponibles sur la machine.
-MaxMem -mm	max_memory_in_mb_to_allocate	Facultatif. Quantité maximale de mémoire en mégaoctets que le service du gestionnaire de ressource peut allouer aux tâches qui s'exécutent sur le nœud de calcul. Un nœud de calcul nécessite au moins 2,5 Go de mémoire pour initialiser un conteneur de façon à démarrer un processus DTM. Par défaut, la mémoire maximale est la mémoire réelle disponible sur la machine.
-ServiceName -sn	service_name	Facultatif. Entrez Resource_Manager_Service.

UpdateServiceOptions

Met à jour les propriétés du service du gestionnaire de ressource. Exécutez cette commande pour configurer le nœud principal et les nœuds de sauvegarde du service du gestionnaire de ressource.

Vous pouvez modifier les propriétés pendant l'exécution du service, mais vous devez redémarrer celui-ci pour que les modifications entrent en vigueur.

La commande `infacmd rms UpdateServiceOptions` utilise la syntaxe suivante :

```
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,...]
```

Le tableau suivant décrit les options et arguments de la commande `infacmd rms UpdateServiceOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Facultatif. Entrez <code>Resource_Manager_Service</code> .
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-Options -o	options	Facultatif. Entrez chaque option en la séparant par un espace.
-NodeName -nn	primary_node_name	Facultatif. Nœud principal sur lequel le service du gestionnaire de ressource s'exécute.
-BackupNodes -bn	backup_node_name1,backup_node_name2,...	Facultatif. Nœuds sur lesquels le service peut s'exécuter si le nœud principal n'est pas disponible.

Options du service du gestionnaire de ressource

Utilisez les options du service du gestionnaire de ressource avec la commande `infacmd rms UpdateServiceOptions`.

Entrez les options du service Metadata Manager au format suivant :

```
... -o option_type.option_name=value
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options du service du gestionnaire de ressource :

Option	Description
ResourceManagerServiceOptions.Log_Level	Niveau des messages d'erreur que le service du gestionnaire de ressource écrit dans le journal du service. Choisissez l'un des niveaux de message suivants : Irrécupérable, Erreur, Avertissement, Informations, Trace ou Déboguer.

CHAPITRE 32

Référence de commande infacmd rtm

Ce chapitre comprend les rubriques suivantes :

- [DeployImport, 1072](#)
- [Exporter, 1074](#)
- [Import, 1077](#)

DeployImport

Importe le contenu d'un fichier d'application vers la base de données lue par le référentiel modèle.

La commande infacmd rtm DeployImport utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd rtm DeployImport :

Option	Argument	Description
-DomainName -dn	Nom de domaine	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	Nom d'utilisateur	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	Mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-securityDomain -sdn	Domaine de sécurité	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	Domain gateway host:port	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Entrez le nom d'hôte et le numéro de port correspondant au nœud de passerelle dans le domaine. Utilisez la syntaxe suivante : gateway_hostname:HttpPort
-NodeName -nn	Nom du nœud	Facultatif. Nom du nœud de passerelle pour le service de référentiel modèle.
-DataIntegrationService -ds	Nom du service d'intégration de données	Requis. Nom du service d'intégration de données.

Option	Argument	Description
-CodePage -cp	Page de code	Requis. Page de code des données de référence à importer.
-Folder -f	Dossier à partir duquel effectuer l'importation	Requis. Chemin vers le dossier contenant les fichiers à importer. Vous devez exécuter la commande DeployImport sur la machine qui stocke le dossier. L'option du dossier décrit un chemin sur la machine qui exécute la commande.
-MetadataFile -mf	Fichier de métadonnées	Requis. Nom complet et chemin du fichier d'application auquel vous appliquez la commande.

Exporter

Exporte les données depuis les tables de référence. Vous pouvez exporter les objets de la table de référence ou seulement les données. Vous pouvez exporter les données depuis les tables de référence gérées et non gérées.

Définit les données d'export à l'aide de l'une des options suivantes :

- ProjectFolder. Nom d'un projet ou d'un dossier à exporter.
- MetadataFile. Nom d'un fichier metadata.xml qui fait référence aux tables de référence à exporter.
- ObjectList. Chemin d'accès complet d'un fichier texte contenant une liste des objets à exporter.

Lorsque vous configurez une liste objet, créez un fichier texte contenant une liste des objets avec la syntaxe suivante :

```
ProjectName/FolderName/reference_table_object1
ProjectName/FolderName/reference_table_object2
ProjectName/FolderName/reference_table_object3
```

Remarque: Chaque chemin d'accès dans la liste objet doit être configuré avec des barres obliques. N'utilisez pas de barre oblique inversée dans le chemin d'accès.

La commande `infacmd rtm Export` utilise la syntaxe suivante :

```
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]

Le tableau suivant décrit les options et arguments d'infacmd rtm Export :

Option	Argument	Description
-DomainName -dn	Nom de domaine	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	Nom d'utilisateur	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	Mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	Domaine de sécurité	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-Gateway -hp	Nom d'hôte de la passerelle de domaine : numéroport	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Entrez le nom d'hôte et le numéro de port correspondant au nœud de passerelle dans le domaine. Utilisez la syntaxe suivante : <code>gateway_hostname:HttpPort</code>
-NodeName -nn	Nom du nœud	Facultatif. Nom du nœud de passerelle pour le service de référentiel modèle.
-RepositoryService -rs	Nom du service de référentiel modèle	Nom du service de référentiel modèle.
-CodePage -cp	Page de code	Requis. Page de code des données de référence.
-Folder -f	Dossier vers lequel effectuer l'exportation	Requis. Emplacement cible du fichier d'exportation.
-ObjectList -ol	Liste des objets à exporter	Nom complet du fichier contenant la liste des objets de la table de référence. Ne pas configurer cette option avec l'option ProjectFolder ou metadataFile.
-ProjectFolder -pf	Nom du dossier du projet à exporter	Nom du projet et du dossier à exporter. Utilisez la syntaxe suivante : <code>ProjectName/FolderName</code> Ne pas configurer cette option avec l'option metadataFile ou ObjectList.
-metadataFile -mf	Fichier de métadonnées	Requis pour l'exportation des objets. Chemin et nom complet d'un fichier metadata.xml auquel vous souhaitez appliquer la commande. Exporte toutes les tables de référence comprises dans les fichiers XML de métadonnées. Ne pas configurer cette option avec l'option ProjectFolder ou ObjectList.
-Recursive -r	Inclure les sous-dossiers lors de l'exportation du dossier du projet	Facultatif. Utiliser avec l'option ProjectFolder. Exporter les objets de plusieurs niveaux. La valeur par défaut n'est pas récursive.
-SkipDatGeneration -sdg	Ignorer la génération de données	Facultatif. Écrit un fichier .dat fichier décrivant la structure de la table de référence dans le répertoire défini dans les propriétés du dossier. Le processus d'importation de la table de référence n'utilise pas ce fichier. La valeur par défaut est False.

Import

Effectue une importation des métadonnées et des données à partir des fichiers d'export d'objets. Importe des métadonnées de table de référence dans le référentiel modèle et importe les données dans la base de données de données de référence. Importe aussi les données de référence sans les métadonnées.

Avant l'importation des données de table de référence, le projet de destination doit exister dans le référentiel modèle.

La commande `infacmd rtm Import` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd rtm Import :

Option	Argument	Description
-DomainName -dn	Nom de domaine	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <i>INFA_DEFAULT_DOMAIN</i> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	Nom d'utilisateur	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <i>INFA_DEFAULT_DOMAIN_USER</i> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	Mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <i>INFA_DEFAULT_DOMAIN_PASSWORD</i> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-securityDomain -sdn	Domaine de sécurité	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <i>INFA_DEFAULT_SECURITY_DOMAIN</i> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Gateway -hp	Domain gateway host:port	Requis si les informations de connectivité de passerelle du fichier domains.infra sont obsolètes. Nom d'hôte et numéro de port du nœud de passerelle dans le domaine. Utilisez la syntaxe suivante : <code>gateway_hostname:HttpPort</code>
-NodeName -nn	Nom du nœud	Facultatif. Nom du nœud de passerelle pour le service de référentiel modèle.
-RepositoryService -rs	Nom du service de référentiel modèle	Requis. Nom du service de référentiel modèle.

Option	Argument	Description
-CodePage -cp	Page de code	Requis. Page de code des données de référence.
-ConflictResolution -cr	Résolution de conflit	<p>Requis. Définit un comportement en cas de conflit de nom. Entrez l'un des arguments suivants :</p> <ul style="list-style-type: none"> - Remplacer. Remplacez l'objet de table de référence actuel par l'objet que vous importez. - Renommer. Créez un objet de table de référence d'un autre nom. - Ignorer. Ne pas importer la table de référence. <p>Remarque: L'argument Replace spécifie la stratégie de résolution pour l'objet table de référence et non pour la table sous-jacente dans la base de données de référence. Lorsque vous utilisez l'argument Replace, la commande Import crée une table pour les données que le nouvel objet représente dans la base de données de référence. La commande n'ignore pas la table identifiée par l'objet précédent.</p> <p>Pour supprimer les tables inutilisées de la base de données des données de référence, exécutez la commande infacmd cms Purge.</p>
-ImportType -it	Type d'import	Requis. Type de contenu à importer. Entrez MetadataAndData pour l'importation de métadonnées et de données.
-Folder -f	Dossier à partir duquel effectuer l'importation	Requis pour l'importation de métadonnées et de données. Chemin d'accès complet au dossier contenant le fichier de données de référence à importer.
-FileName -fn	Requis uniquement pour l'importation d'un dictionnaire unique	Requis pour l'importation de métadonnées et de données si elle se fait à partir d'un seul fichier. Nom du fichier contenant les données de référence à importer. Le nom du fichier correspond au chemin du dossier.
-MetadataFile -mf	Requis uniquement pour l'importation d'un objet	Requis uniquement lors de l'importation de valeurs de données de référence. Chemin et nom complet du fichier metadata.xml auquel vous appliquez la commande. Le fichier metadata.xml contient les métadonnées associées aux valeurs de données de référence. Ne pas utiliser cette option avec l'option ProjectFolder.
-ProjectFolder -pf	Nom du dossier du projet dans lequel effectuer l'importation	Requis lorsque vous importez des données de référence et des métadonnées. Nom du projet de référentiel modèle dans lequel vous souhaitez effectuer l'importation. Ne pas utiliser cette option avec l'option MetadataFile.
-NotRecursive -nr	- Ne pas inclure les sous-dossiers	Facultatif. Utiliser cette option avec l'importation de métadonnées et de données. Importe uniquement un niveau d'objets. La valeur par défaut est récursive.

CHAPITRE 33

Référence de commande infacmd sch

Ce chapitre comprend les rubriques suivantes :

- [CreateSchedule, 1080](#)
- [DeleteSchedule, 1087](#)
- [ListSchedule, 1088](#)
- [ListServiceOptions, 1090](#)
- [ListServiceProcessOptions, 1090](#)
- [PauseAll, 1092](#)
- [PauseSchedule, 1092](#)
- [ResumeAll, 1093](#)
- [ResumeSchedule, 1094](#)
- [UpdateSchedule, 1095](#)
- [UpdateServiceOptions, 1098](#)
- [UpdateServiceProcessOptions, 1101](#)
- [Mise à niveau, 1103](#)

CreateSchedule

Crée une planification pour les mappages et les flux de travail déployés.

La syntaxe de la commande infacmd sch CreateSchedule est la suivante :

```
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]

```

Pour configurer plusieurs valeurs d'un argument, séparez les valeurs par des virgules.

Le tableau suivant décrit les options et arguments d'infacmd sch CreateSchedule :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine.
-ScheduleName -scn	schedule_name	Obligatoire. Nom de la planification. Le nom de la planification est sensible à la casse.
-Description -scd	schedule_description	Facultatif. Description de la planification.

Option	Argument	Description
-Recurrence -r	une fois quotidienne hebdomadaire mensuelle	Obligatoire. Indiquez si la planification s'exécute une fois ou si elle se reproduit.
-StartTime -st	yyyy-MM-dd HH:mm	Obligatoire. Date et heure auxquelles la récurrence démarre.
-EndTime -et	yyyy-MM-dd HH:mm	Facultatif. Date et heure auxquelles la récurrence se termine.
-TimeZone -tz	timezone	Facultatif. Fuseau horaire de l'heure de début de la planification. Pour configurer le fuseau horaire, vous pouvez entrer le numéro d'identifiant du fuseau horaire ou l'identifiant de base de données Olson. La valeur par défaut correspond aux paramètres régionaux de la machine du client.
-DailyRunEvery -dre	daily_run_every	Facultatif. Exécute la planification selon un intervalle. La liste suivante décrit les options que vous pouvez configurer : <ul style="list-style-type: none"> - minute(s). Exécute le programme chaque jour toutes les n minutes. - heure(s). Exécute le programme chaque jour toutes les n heures. - jour(s). Exécute la planification tous les n jours. - semaine(s). Exécute la planification toutes les n semaines. - mois. Exécute la planification tous les n mois. - année(s). Exécute la planification tous les n ans. - FIRST. Exécute la planification chaque premier n jour du mois. Utilisez l'option -rdwm pour spécifier le jour ou les jours de la semaine. - SECOND. Exécutez la planification tous les deuxième n jour du mois. Utilisez l'option -rdwm pour spécifier le jour ou les jours de la semaine. - THIRD. Exécutez la planification tous les troisième n jour du mois. Utilisez l'option -rdwm pour spécifier le jour ou les jours de la semaine. - FOURTH. Exécutez la planification tous les quatrième n jour du mois. Utilisez l'option -rdwm pour spécifier le jour ou les jours de la semaine. - LAST. Exécutez la planification tous les derniers n jour du mois. Utilisez l'option -rdwm pour spécifier le jour ou les jours de la semaine.
-RunDaysOfWeek -rdw	lun mar mer jeu ven sam dim	Facultatif. Exécutez la planification certaines jours de la semaine.
-RunDayOfWeekMonth -rdwm	lundi mardi mercredi jeudi vendredi samedi dimanche	Facultatif. Exécutez la planification certains jours de la semaine chaque mois. Utilisez les options -dre pour exécuter la planification chaque premier, deuxième, troisième, quatrième ou dernier n jour du mois.
-RunDayofMonth -rdm	1-30 LAST_DAY_OF_MONTH	Facultatif. Exécutez la planification le n du mois.

Option	Argument	Description
-RepeatCount -rc	repeat_count	Facultatif. Terminez la récurrence après un certain nombre d'exécutions et pas à une date spécifique.
-RunnableObjects -ro	runnableObjects	<p>Facultatif. Objets que vous souhaitez planifier. Entrez le type d'objet, suivi du chemin de l'objet dans le service d'intégration de données. Par exemple :</p> <pre>"workflow://DIS_hw2288/App_DMPA_run/wf_run_DMPA"</pre> <p>Vous pouvez éventuellement utiliser les arguments suivants pour configurer un fichier de paramètres, un ensemble de paramètres ou l'exécution de l'objet en tant qu'utilisateur ou profil de système d'exploitation :</p> <ul style="list-style-type: none"> - parameterFilePath=PATH_TO_PARAMETER_FILE - parameterSet=PARAMETER_SET_NAME - runAsUser=USER_NAME &runAsUserSecurityDomain=SECURITY_DOMAIN &runAsUserPassword=PASSWORD - osProfileName=OS_PROFILE_NAME <p>Par exemple :</p> <pre>"workflow:DIS_1234/Application_workflow/Workflow_abc?parameterFilePath=C://Informatica/ParameterFiles/Parameter.xml&runAsUser=Administrator&runAsUserSecurityDomain=Native&runAsUserPassword=Administrator"</pre>
-Status -ss	SCHEDULED PAUSED	Facultatif. Créez la planification à l'état planifié ou en pause.
-RunNow -rn	true false	Exécutez la planification immédiatement.

Paramètres de fuseau horaire valides

Lorsque vous entrez le paramètre de fuseau horaire, vous pouvez entrer un ID de fuseau horaire ou l'ID de base de données Olson.

Le tableau suivant répertorie les valeurs que vous pouvez entrer pour le fuseau horaire :

ID	ID de base de données Olson	Nom
0	Etc/GMT+12	(UTC-12:00) Ouest de la ligne de changement de date
110	Etc/GMT+11	(UTC-11:00) Temps universel coordonné -11
200	Pacifique/Honolulu	(UTC-10:00) Hawaï
300	Amérique/Anchorage	(UTC-09:00) Alaska

ID	ID de base de données Olson	Nom
410	Amérique/Santa Isabel	(UTC-08:00) Basse-Californie
400	Amérique/Los Angeles	(UTC-08:00) Heure du Pacifique (États-Unis-et Canada)
520	Amérique/Phoenix	(UTC-07:00) Arizona
510	Amérique/Chihuahua	(UTC-07:00) Chihuahua, La Paz, Mazatlan
500	Amérique/Denver	(UTC-07:00) Rocheuses (États-Unis-et Canada)
610	Amérique/Guatemala	(UTC-06:00) Amérique centrale
620	Amérique/Chicago	(UTC-06:00) Heure du Centre (États-Unis-et Canada)
630	Amérique/Mexico	(UTC-06:00) Guadalajara, Mexico, Monterrey
600	Amérique/Regina	(UTC-06:00) Saskatchewan
710	Amérique/Bogota	(UTC-05:00) Bogota, Lima, Quito, Rio Branco
700	Amérique/New York	(UTC-05:00) Heure de l'Est (États-Unis-et Canada)
720	Amérique/Indianapolis	(UTC-05:00) Indiana (Est)
840	Amérique/Caracas	(UTC-04:30) Caracas
850	Amérique/Asuncion	(UTC-04:00) Asuncion
800	Amérique/Halifax	(UTC-04:00) Heure de l'Atlantique (Canada)
810	Amérique/Cuiaba	(UTC-04:00) Cuiaba
830	Amérique/La Paz	(UTC-04:00) Georgetown, La Paz, Manaus, San Juan
900	Amérique/Saint-Jean	(UTC-03:30) Terre-Neuve
910	Amérique/Sao Paulo	(UTC-03:00) Brasilia
940	Amérique/Cayenne	(UTC-03:00) Cayenne, Fortaleza
950	Amérique/Buenos Aires	(UTC-03:00) Buenos Aires
920	Amérique/Godthab	(UTC-03:00) Groenland
930	Amérique/Montevideo	(UTC-03:00) Montevideo
820	Amérique/Santiago	(UTC-03:00) Santiago
1010	Etc/GMT+2	(UTC-02:00) Temps universel coordonné -02
1100	Atlantique/Açores	(UTC-01:00) Açores
1110	Atlantique/Cap Vert	(UTC-01:00) Îles du Cap Vert

ID	ID de base de données Olson	Nom
1220	Afrique/Casablanca	(UTC) Casablanca
1230	Etc/GMT	(UTC) Temps universel coordonné
1200	Europe/Londres	(UTC) Dublin, Édimbourg, Lisbonne, Londres
1210	Atlantique/Reykjavik	(UTC) Monrovia, Reykjavik
1340	Europe/Berlin	(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienne
1300	Europe/Budapest	(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
1320	Europe/Paris	(UTC+01:00) Bruxelles, Copenhague, Madrid, Paris
1310	Europe/Varsovie	(UTC+01:00) Sarajevo, Skopje, Varsovie, Zagreb
1330	Afrique/Lagos	(UTC+01:00) Afrique Centrale et Occidentale
1350	Afrique/Windhoek	(UTC+01:00) Windhoek
1450	Asie/Amman	(UTC+02:00) Amman
1430	Europe/Bucarest	(UTC+02:00) Athènes, Bucarest
1460	Asie/Beyrouth	(UTC+02:00) Beyrouth
1410	Afrique/Le Caire	(UTC+02:00) Le Caire
1480	Asie/Damas	(UTC+02:00) Damas
1470	Afrique/Johannesburg	(UTC+02:00) Harare, Pretoria
1420	Europe/Kiev	(UTC+02:00) Helsinki, Kiev, Riga, Sofia, Tallinn, Vilnius
1490	Europe/Istanbul	(UTC+02:00) Istanbul
1440	Asie/Jérusalem	(UTC+02:00) Jérusalem
1530	Europe/Kaliningrad	(UTC+02:00) Kaliningrad (RTZ 1)
1510	Asie/Bagdad	(UTC+03:00) Bagdad
1500	Asie/Riyad	(UTC+03:00) Koweït, Riyad
1400	Europe/Minsk	(UTC+03:00) Minsk
1540	Europe/Moscou	(UTC+03:00) Moscou, Saint-Pétersbourg, Volgograd (RTZ 2)
1520	Afrique/Nairobi	(UTC+03:00) Nairobi
1550	Asie/Téhéran	(UTC+03:30) Téhéran

ID	ID de base de données Olson	Nom
1600	Asie/Dubaï	(UTC+04:00) Abu Dhabi, Mascate
1610	Asie/Bakou	(UTC+04:00) Bakou
1650	Inde/Maurice	(UTC+04:00) Port Louis
1640	Asie/Tbilissi	(UTC+04:00) Tbilissi
1620	Asie/Erevan	(UTC+04:00) Erevan
1630	Asie/Kaboul	(UTC+04:30) Kaboul
1710	Asie/Tachkent	(UTC + 05:00) Achgabat, Tachkent
1700	Asie/Iekaterinbourg	(UTC+05:00) Iekaterinbourg (RTZ 4)
1750	Asie/Karachi	(UTC+05:00) Islamabad, Karachi
1720	Asie/Calcutta	(UTC+05:30) Chennai, Calcutta, Bombay, New Delhi
1730	Asie/Colombo	(UTC+05:30) Sri Jayawardenepura Kotte
1740	Asie/Katmandou	(UTC+05:45) Katmandou
1800	Asie/Almaty	(UTC+06:00) Astana
1830	Asie/Dacca	(UTC+06:00) Astana
1810	Asie/Novossibirsk	(UTC+06:00) Novossibirsk (RTZ 5)
1820	Asie/Rangoun	(UTC+06:30) Rangoun
1910	Asie/Bangkok	(UTC+07:00) Bangkok, Hanoï, Djakarta
1900	Asie/Krasnoïarsk	(UTC+07:00) Krasnoïarsk (RTZ 6)
2000	Asie/Shanghai	(UTC+08:00) Pékin, Chongqing, Hong Kong, Ürümqi
2010	Asie/Irkoutsk	(UTC+08:00) Irkoutsk (RTZ 7)
2020	Asie/Singapour	(UTC+08:00) Kuala Lumpur, Singapour
2040	Australie/Perth	(UTC+08:00) Perth
2030	Asie/Taipei	(UTC+08:00) Taipei
2050	Asie/Oulan-Bator	(UTC+08:00) Oulan-Bator
2110	Asie/Tokyo	(UTC+09:00) Osaka, Sapporo, Tokyo
2100	Asie/Séoul	(UTC+09:00) Séoul
2120	Asie/Iakoutsk	(UTC+09:00) Iakoutsk (RTZ 8)

ID	ID de base de données Olson	Nom
2140	Australie/Adélaïde	(UTC+09:30) Adélaïde
2130	Australie/Darwin	(UTC+09:30) Darwin
2210	Australie/Brisbane	(UTC+10:00) Brisbane
2200	Australie/Sydney	(UTC+10:00) Canberra, Melbourne, Sydney
2240	Pacifique/Port Moresby	(UTC+10:00) Guam, Port Moresby
2220	Australie/Hobart	(UTC+10:00) Hobart
2310	Asie/Magadan	(UTC+10:00) Magadan
2230	Asie/Vladivostok	(UTC+10:00) Vladivostok, Magadan (RTZ 9)
2300	Pacifique/Guadalcanal	(UTC+11:00) Îles Salomon, Nouvelle-Calédonie
2410	Pacifique/Auckland	(UTC+12:00) Auckland, Wellington
2430	Etc/GMT-12	(UTC+12:00) Temps universel coordonné +12
2400	Pacifique/Fidji	(UTC+12:00) Îles Fidji
2500	Pacifique/Tongatapu	(UTC+13:00) Nuku'alofa
2510	Pacifique/Apia	(UTC+13:00) Samoa

DeleteSchedule

Supprime une ou plusieurs planifications gérées par le service de planificateur.

La commande `infacmd sch DeleteSchedule` utilise la syntaxe suivante :

```

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

```

Le tableau suivant décrit les options et les arguments de la commande `infacmd sch DeleteSchedule` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine.
-ScheduleName -scn	schedule_name	Nom de la planification à supprimer.

ListSchedule

Répertorie les planifications ou les objets planifiés gérés par le service de planificateur. La commande renvoie les planifications ou les objets planifiés qui correspondent à toutes les options entrées.

La commande `infacmd sch ListSchedule` utilise la syntaxe suivante :

```
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]

Le tableau suivant décrit les options et les arguments de la commande infacmd isp ListSchedule :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine.
ScheduleName -scn	schedule_name	Facultatif. Renvoie les planifications portant le nom n.
Description -scd	description	Facultatif. Renvoie les planifications portant la description n.
RunnableObjects -ro	runnableObjects	Facultatif. Répertorie les planifications qui exécutent un objet. Entrez le type d'objet et le chemin sur le service d'intégration de données dans le format suivant : '{mapping workflow}://dis_name/app_name/obj_name' Par exemple : 'mapping://dis_demo/app_demo/mapping_demo'
ScheduleStatus -ss	créé planifié en pause terminé	Facultatif. Renvoie les planifications dont le statut est n.
NumberOfFireTimes -n	number_of_fire_times	Facultatif. Renvoie les planifications qui ont été exécutées n fois.
Maxresults -m	max_results	Facultatif. Nombre maximal de planifications que la commande doit exécuter.

ListServiceOptions

Renvoie une liste de propriétés qui sont configurées pour le service de planificateur.

La commande `infacmd sch ListServiceOptions` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd sch ListServiceOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-ServiceName -sn	service_name	Requis. Entrez Scheduler_Service.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine.

ListServiceProcessOptions

Renvoie une liste de propriétés qui sont configurés pour un processus de service de planificateur.

La commande `infacmd sch ListServiceProcessOptions` utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et les arguments de la commande `infacmd sch ListServiceProcessOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-ServiceName -sn	service_name	Requis. Entrez Scheduler_Service.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine.
-NodeName -nn	node_name	Nom du nœud sur lequel le processus de service s'exécute.

PauseAll

Suspend toutes les planifications gérées par le service de planificateur. Lorsque vous suspendez les planifications, les objets qui s'exécutent selon les planifications s'interrompent jusqu'à ce que vous repreniez les planifications.

La commande `infacmd sch PauseAll` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd sch PauseAll` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine.

PauseSchedule

Suspend une planification gérée par le service de planificateur. Lorsque vous suspendez une planification, les objets qui s'exécutent selon cette planification s'arrêtent jusqu'à ce que vous repreniez la planification.

La commande `infacmd sch PauseSchedule` utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et les arguments de la commande `infacmd sch PauseSchedule` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine.
-ScheduleName -scn	schedule_name	Nom de la planification que vous voulez suspendre. Le nom de la planification est sensible à la casse.

ResumeAll

Reprend toutes les planifications suspendues gérées par le service de planificateur.

La commande `infacmd sch ResumeAll` utilise la syntaxe suivante :

```

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]

```

Le tableau suivant décrit les options et les arguments de la commande `infacmd sch ResumeAll` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine.

ResumeSchedule

Reprend une planification suspendue gérée par le service de planificateur.

La commande `infacmd sch ResumeSchedule` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd sch ResumeSchedule` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine

Option	Argument	Description
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier domains.infa sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine.
ScheduleName -scn	schedule_name	Nom de la planification suspendue que vous voulez reprendre.

UpdateSchedule

Met à jour une planification gérée par le service de planificateur. Mettez à jour une planification afin d'en modifier les heures de début ou de fin, la récurrence ou les objets qui s'exécutent selon la planification. Pour afficher les options actuelles, exécutez la commande `infacmd sch ListSchedule`.

La commande `infacmd sch UpdateSchedule` utilise la syntaxe suivante :

```
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]
```

Pour configurer plusieurs valeurs d'un argument, séparez les valeurs par des virgules.

Le tableau suivant décrit les options et les arguments de la commande `infacmd sch UpdateSchedule` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine.
-ScheduleName -scn	schedule_name	Obligatoire. Nom de la planification. Le nom de la planification est sensible à la casse.
-Description -scd	schedule_description	Facultatif. Description de la planification.
-Recurrence -r	une fois quotidienne hebdomadaire mensuelle	Obligatoire. Indiquez si la planification s'exécute une fois ou si elle se reproduit.
-StartTime -st	yyyy-MM-dd HH:mm	Obligatoire. Date et heure auxquelles la récurrence démarre.
-EndTime -et	yyyy-MM-dd HH:mm	Facultatif. Date et heure auxquelles la récurrence se termine.
-TimeZone -tz	timezone	Facultatif. Fuseau horaire de l'heure de début de la planification. Pour configurer le fuseau horaire, vous pouvez entrer le numéro d'identifiant du fuseau horaire ou l'identifiant de base de données Olson. La valeur par défaut correspond aux paramètres régionaux de la machine du client.

Option	Argument	Description
-DailyRunEvery -dre	daily_run_every	Facultatif. Exécute la planification selon un intervalle. La liste suivante décrit les options que vous pouvez configurer : <ul style="list-style-type: none"> - minute(s). Exécute le programme chaque jour toutes les n minutes. - heure(s). Exécute le programme chaque jour toutes les n heures. - jour(s). Exécute la planification tous les n jours. - semaine(s). Exécute la planification toutes les n semaines. - mois. Exécute la planification tous les n mois. - année(s). Exécute la planification tous les n ans. - FIRST. Exécute la planification chaque premier n jour du mois. Utilisez l'option -rdwm pour spécifier le jour ou les jours de la semaine. - SECOND. Exécutez la planification tous les deuxième n jour du mois. Utilisez l'option -rdwm pour spécifier le jour ou les jours de la semaine. - THIRD. Exécutez la planification tous les troisième n jour du mois. Utilisez l'option -rdwm pour spécifier le jour ou les jours de la semaine. - FOURTH. Exécutez la planification tous les quatrième n jour du mois. Utilisez l'option -rdwm pour spécifier le jour ou les jours de la semaine. - LAST. Exécutez la planification tous les derniers n jour du mois. Utilisez l'option -rdwm pour spécifier le jour ou les jours de la semaine.
-RunDaysOfWeek -rdw	lun mar mer jeu ven sam dim	Facultatif. Exécutez la planification certaines jours de la semaine.
-RunDayOfWeekMonth -rdwm	lundi mardi mercredi jeudi vendredi samedi dimanche	Facultatif. Exécutez la planification certains jours de la semaine chaque mois. Utilisez les options -dre pour exécuter la planification chaque premier, deuxième, troisième, quatrième ou dernier n jour du mois.
-RunDayOfMonth -rdm	1-30 LAST_DAY_OF_MONTH	Facultatif. Exécutez la planification le n du mois.
-RepeatCount -rc	repeat_count	Facultatif. Terminez la récurrence après un certain nombre d'exécutions et pas à une date spécifique.

Option	Argument	Description
RemoveRunnableObjects -rro	removeRunnableObjects	Facultatif. Retire les objets de la planification. Entrez les objets au format suivant : <pre>"{mapping workflow}:Data Integration Service/ Application/{Mapping Workflow}[[?]] [parameterFilePath=PATH_TO_PARAMETER_FILE parameterSet=PARAMETER_SET_NAME] &runAsUser=USER_NAME &runAsUserSecurityDomain=SECURITY_DOMAIN &runAsUserPassword=PASSWORD]]"]</pre>
-AddRunnableObjects -aro	addRunnableObjects	Facultatif. Ajoute des objets à la planification. Objets que vous souhaitez planifier. Entrez le type d'objet, suivi du chemin de l'objet dans le service d'intégration de données. Par exemple : <pre>"mapping:DIS_1234/Application_mapping/ Mapping_abc"</pre> <p>Vous pouvez éventuellement utiliser les arguments suivants pour configurer un fichier de paramètres, un ensemble de paramètres ou l'exécution de l'objet en tant qu'utilisateur ou profil de système d'exploitation :</p> <ul style="list-style-type: none"> - parameterFilePath=PATH_TO_PARAMETER_FILE - parameterSet=PARAMETER_SET_NAME - runAsUser=USER_NAME &runAsUserSecurityDomain=SECURITY_DOMAIN &runAsUserPassword=PASSWORD - osProfileName=OS_PROFILE_NAME <p>Par exemple :</p> <pre>"workflow:DIS_1234/Application_workflow/ Workflow_abc?parameterFilePath= C://Informatica/Parameter Files/Parameter.xml &runAsUser=Administrator &runAsUserSecurityDomain=Native &runAsUserPassword=Administrator"</pre>

Pour une liste des valeurs de fuseau horaire valides, consultez ["Paramètres de fuseau horaire valides" à la page 1083](#).

UpdateServiceOptions

Mettez à jour les propriétés du service de planificateur. Pour afficher les options actuelles, exécutez la commande `infacmd sch ListServiceOptions`.

La commande `infacmd sch UpdateServiceOptions` utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et les arguments de la commande `infacmd sch UpdateServiceOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-ServiceName -sn	service_name	Requis. Entrez Scheduler_Service.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine.
-NodeName -nn	primary node name	Facultatif. Nœud principal sur lequel le service s'exécute.
-BackupNodes -bn	node_name1,node_name2,...	Facultatif. Nœuds sur lesquels le service peut s'exécuter si le nœud principal n'est pas disponible.
Options -o	options	Facultatif. Entrez chaque option en la séparant par un espace.

Options du service de planificateur

Utilisez les options du service de planificateur avec la commande `infacmd sch UpdateServiceOptions`.

Entrez les options du service de planificateur au format suivant :

```
... -o option_type.option_name=value
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options du service de planificateur :

Option	Description
<code>SchedulerPersistenceOptions.SchedulerRepositoryServiceName</code>	Service de référentiel modèle associé au service de planificateur.
<code>SchedulerPersistenceOptions.SchedulerRepositoryUsername</code>	Nom d'utilisateur d'un administrateur dans le domaine Informatica. Non disponible pour un domaine avec l'authentification Kerberos.
<code>SchedulerPersistenceOptions.SchedulerRepositoryPassword</code>	Mot de passe de l'administrateur dans le domaine Informatica. Non disponible pour un domaine avec l'authentification Kerberos.
<code>SchedulerPersistenceOptions.SchedulerRepositorySecurityDomain</code>	Domaine de sécurité LDAP pour l'utilisateur qui gère le service de planificateur. Le champ Domaine de sécurité ne s'affiche pas pour les utilisateurs ayant l'authentification native ou Kerberos.

Option	Description
SchedulerLoggingOptions.SchedulerLogLevel	<p>Détermine le niveau de gravité par défaut des journaux de service. Choisissez l'une des options suivantes :</p> <ul style="list-style-type: none"> - Fatal. Consigne des messages FATAL dans le journal. Les messages FATAL incluent notamment les défaillances du système irrécupérables qui entraînent l'arrêt ou l'indisponibilité du service. - Erreur. Consigne des messages FATAL et ERROR dans le journal. Les messages ERROR incluent notamment les échecs de connexion, les échecs d'enregistrement ou de récupération des métadonnées et les erreurs de service. - Avertissement. Consigne des messages FATAL, WARNING et ERROR dans le journal. Les erreurs WARNING incluent notamment les avertissements ou les défaillances du système récupérables. - Info. Consigne des messages FATAL, INFO, WARNING, et ERROR dans le journal. Les messages INFO incluent notamment les messages de modification du système et du service. - Suivi. Consigne des messages FATAL, TRACE, INFO, WARNING et ERROR dans le journal. Les messages TRACE enregistrent les échecs des demandes de l'utilisateur. - Débogage. Consigne des messages FATAL, DEBUG, TRACE, INFO, WARNING et ERROR dans le journal. Les messages DEBUG sont les journaux des demandes de l'utilisateur.
SchedulerStorageOptions.SchedulerTempFileLocation	<p>Chemin du répertoire où les fichiers de paramètres permettent la lecture et l'écriture. Configurez l'emplacement de fichier temporaire sur un répertoire accessible à tous les nœuds du domaine.</p>

UpdateServiceProcessOptions

Met à jour les propriétés d'un processus de service de planificateur. Pour afficher la configuration du processus en cours, exécutez la commande `infacmd sch ListServiceProcessOptions`.

La commande `infacmd sch UpdateServiceProcessOptions` utilise la syntaxe suivante:

```
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
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd sch UpdateServiceProcessOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-ServiceName -sn	service_name	Requis. Entrez Scheduler_Service.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine.
NodeName -nn	node_name	Nom du nœud sur lequel le processus de service s'exécute.
Options -o	options	Facultatif. Entrez chaque option en la séparant par un espace.

Options du processus de service de planificateur

Utilisez les options du service de planificateur avec la commande `infacmd sch UpdateServiceOptions`.

Entrez les options du service de planificateur au format suivant :

```
... -o option_type.option_name=value
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options du service de planificateur :

Option	Description
<code>SchedulerServiceAdvancedOptions.JVMOptions</code>	Options de ligne de commande de la machine virtuelle Java (JVM) pour l'exécution de programmes Java. Lorsque vous configurez les options JVM, vous devez définir le chemin de classe, ainsi que la mémoire minimale et maximale Java SDK. Vous devez définir les options de ligne de commande JVM suivantes : <ul style="list-style-type: none">- <code>Xms</code>. Taille minimum du tas mémoire. La valeur par défaut est 256 m.- <code>MaxPermSize</code>. Taille de génération permanente maximum. La valeur par défaut est 128 m.- <code>Dfile.encoding</code>. Codage de fichier. La valeur par défaut est UTF-8.
<code>HttpConfigurationOptions.KeyStoreFile</code>	Chemin et nom du fichier keystore qui contient les clés et les certificats. Requis si vous utilisez des connexions HTTPS pour le service. Vous pouvez créer un fichier keystore à l'aide d'un utilitaire <code>keytool</code> . <code>Keytool</code> est un utilitaire qui génère et stocke des paires de clés privées ou publiques et les certificats associés dans un fichier keystore. Vous pouvez utiliser le certificat auto-signé ou un certificat signé par une autorité de certification.
<code>HttpConfigurationOptions.KeyStorePassword</code>	Mot de passe du fichier keystore.
<code>HttpConfigurationOptions.TrustStoreFile</code>	Chemin et nom du fichier truststore contenant les certificats d'authentification approuvés par le service.
<code>HttpConfigurationOptions.TrustStorePassword</code>	Mot de passe du fichier keystore.
<code>HttpConfigurationOptions.SSLProtocol</code>	Protocole Secure Sockets Layer à utiliser. La valeur par défaut est TLS.
<code>SchedulerServiceSecurityOptions.HttpPort</code>	Numéro de port HTTP unique pour le processus de service de planificateur lorsque le service utilise le protocole HTTP. La valeur par défaut est 6211.
<code>SchedulerServiceSecurityOptions.HttpsPort</code>	Numéro de port HTTPS unique pour le processus de service de planificateur lorsque le service utilise le protocole HTTPS. Lorsque vous définissez un numéro de port HTTPS, vous devez également définir le fichier keystore qui contient les clés et les certificats.

Mise à niveau

Met à niveau la configuration du service de planificateur. Exécutez la commande `sch Upgrade` lorsque vous mettez à niveau vers la version actuelle d'Informatica.

La commande `infacmd sch Upgrade` utilise la syntaxe suivante :

```
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]

```

Le tableau suivant décrit les options et les arguments de la commande `infacmd sch Upgrade` :

Option	Argument	Description
-DomainName -dn	domain_name	Nom du domaine Informatica.
-ServiceName -sn	service_name	Requis. Entrez Scheduler_Service.
-UserName -un	user_name	Nom d'utilisateur pour se connecter au domaine
-Password -pd	mot de passe	Mot de passe pour le nom d'utilisateur.
-SecurityDomain -sdn	security_domain	Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Requis si les informations de connectivité de passerelle du fichier <code>domains.infa</code> sont obsolètes. Noms d'hôte et numéros de port pour les nœuds de passerelle du domaine.
-ResilienceTimeout -re	timeout_period_in_seconds	Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine.

CHAPITRE 34

Référence de commande infacmd search

Ce chapitre comprend les rubriques suivantes :

- [CreateService, 1105](#)
- [ListServiceOptions, 1108](#)
- [ListServiceProcessOptions, 1110](#)
- [UpdateServiceOptions, 1111](#)
- [UpdateServiceProcessOptions, 1113](#)

CreateService

Crée un service de recherche. Par défaut, le service de recherche est activé lorsque vous le créez.

La commande `infacmd search CreateService` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd search CreateService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-NodeName -nn	node_name	Obligatoire. Nœud sur lequel le service de recherche s'exécute.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-ServiceName -sn	service_name	Obligatoire. Nom du service de recherche. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 230 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-FolderPath -fp	full_folder_path	Facultatif. Chemin d'accès complet, sans le nom de domaine, du dossier dans lequel vous souhaitez ajouter le service de recherche. Doit être au format suivant : /parent_folder/child_folder La valeur par défaut est « / » (le domaine).
-BackupNodes -bn	node_name1,node_name2,...	Facultatif. Nœuds sur lesquels le processus de service peut s'exécuter lorsque le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.
-SearchServicePort -sp	search_service_port_number	Obligatoire. Port sur lequel est exécuté le service de recherche.
-IndexLocation -il	search_index_location	Répertoire contenant les fichiers d'index de la recherche.
-ExtractionInterval -ei	search_extraction_interval	Intervalle en secondes selon lequel le service de recherche met à jour l'index de recherche.
-RepositoryService -rsn	model_repository_service_name	Service de référentiel modèle à associer au service de recherche. Le service de référentiel modèle ne peut pas être affecté à un autre service de recherche.
-searchUserName -sun	username_for_search_repositories	Nom d'utilisateur pour l'accès au service de référentiel modèle. L'utilisateur du référentiel modèle doit disposer du rôle d'administrateur.

Option	Argument	Description
-searchPassword -spd	password_for_search_repositories	Mot de passe utilisateur pour l'accès au service de référentiel modèle.
-searchSecurityDomain -ssdn	security_domain_of_search_repositories	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel appartient l'utilisateur du référentiel modèle. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

ListServiceOptions

Répertorie les propriétés d'un service de recherche.

La commande `infacmd search ListServiceOptions` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'`infacmd search ListServiceOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-NodeName -nn	node_name	Obligatoire. Nœud sur lequel le service de recherche s'exécute.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-UserName -un	user_name	<p>Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>
-Password -pd	mot de passe	<p>Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p>
-ServiceName -sn	service_name	Obligatoire. Nom du service de recherche.
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>

ListServiceProcessOptions

Répertorie les propriétés d'un processus de service de recherche.

La commande infacmd search ListServiceProcessOptions utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd search ListServiceProcessOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-NodeName -nn	node_name	Obligatoire. Nom de nœud où le processus de service s'exécute.
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>

Option	Argument	Description
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de recherche.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

UpdateServiceOptions

Met à jour les propriétés du service de recherche. Pour afficher les propriétés actuelles, exécutez la commande `infacmd search ListServiceOptions`.

Vous pouvez changer les propriétés lorsque le service est en cours d'exécution. Toutefois, vous devez recycler le service pour que les changements soient pris en compte.

La commande `infacmd search UpdateServiceOptions` utilise la syntaxe suivante :

```
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,...]

```

Le tableau suivant décrit les options et arguments de la commande `infacmd search UpdateServiceOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de recherche.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Options -o	options	Facultatif. Entrez chaque option en la séparant par un espace. Place une valeur d'option entre guillemets doubles si elle contient un espace. Pour afficher des options, exécutez la commande infacmd search ListServiceOptions.
-NodeName -nn	nom du nœud	Facultatif. Nœud sur lequel le service de recherche s'exécute.
-BackupNodes -bn	node_name1,node_name2,.. ..	Facultatif. Nœuds sur lesquels le processus de service peut s'exécuter lorsque le nœud principal n'est pas disponible. Vous pouvez configurer les nœuds de sauvegarde si vous bénéficiez de la haute disponibilité.

UpdateServiceProcessOptions

Met à jour les propriétés d'un processus de service de recherche. Pour afficher les propriétés actuelles, exécutez la commande infacmd search ListServiceProcessOptions.

Entrez les options de connexion au format suivant :

```
... -o option_name=value option_name=value ...
```

Séparez les options multiples par un espace. Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

La commande infacmd search UpdateServiceProcessOptions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments de la commande `infacmd search`
`UpdateServiceProcessOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
NodeName -nn	node_name	Obligatoire. Nœud sur lequel le service de recherche s'exécute.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service de recherche.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Options -o	options	Obligatoire. Entrez chaque option en la séparant par un espace. Pour afficher les options, exécutez la commande infacmd search ListServiceProcessOptions.

CHAPITRE 35

Référence de commande infacmd sql

Ce chapitre comprend les rubriques suivantes :

- [ExecuteSQL, 1117](#)
- [ListColumnOptions, 1117](#)
- [ListColumnPermissions, 1119](#)
- [ListSQLDataServiceOptions, 1121](#)
- [ListSQLDataServicePermissions, 1123](#)
- [ListSQLDataServices, 1124](#)
- [ListStoredProcedurePermissions, 1126](#)
- [ListTableOptions, 1127](#)
- [ListTablePermissions, 1129](#)
- [PurgeTableCache, 1131](#)
- [RefreshTableCache , 1133](#)
- [RenameSQLDataService, 1134](#)
- [SetColumnPermissions, 1136](#)
- [SetSQLDataServicePermissions, 1138](#)
- [SetStoredProcedurePermissions, 1141](#)
- [SetTablePermissions, 1143](#)
- [StartSQLDataService, 1146](#)
- [StopSQLDataService, 1148](#)
- [UpdateColumnOptions, 1150](#)
- [UpdateSQLDataServiceOptions, 1152](#)
- [UpdateTableOptions, 1156](#)

ExecuteSQL

Exécute les instructions SQL qui accèdent à un service de données SQL.

Exécutez la commande `infacmd sql ExecuteSQL` en mode interactif ou non interactif. Lorsque vous exécutez `ExecuteSQL` en mode interactif, vous pouvez entrer les instructions SQL sans écrire un script. Lorsque vous utilisez le mode interactif, entrez la chaîne de connexion sans l'option `-Sql`. Vous pouvez exécuter les instructions SQL suivantes sans entrer les informations de connexion pour chaque instruction.

La commande `infacmd sql ExecuteSQL` utilise la syntaxe suivante :

```
ExecuteSQL
<-ConnectionString|-cs> connection_string
[<-Sql> sql_statement]
```

Le tableau suivant décrit les options et arguments d'`infacmd sql ExecuteSQL` :

Option	Argument	Description
<code>-ConnectionString</code> <code>-cs</code>	<code>connection_string</code>	<p>Obligatoire. Entrez une chaîne de connexion au service de données SQL avec la syntaxe suivante :</p> <pre>jdbc:informatica:sqllds/ <optional security domain\> <optional user name>/ <optional user password>@ <domain host name>: <domain HTTP port>?dis= <Data Integration Service name>&sqllds= <runtime SQL data service name></pre> <p>Éventuellement, ajoutez des options dans le format suivant :</p> <pre>... &<option_name>=<option_value></pre> <p>La chaîne de connexion a l'option et la valeur suivantes : SQLDataServiceOptions.disableResultSetCache=true</p> <p>Désactive la mise en cache de l'ensemble de résultats pour une requête de service de données SQL lorsque le service de données SQL est configuré pour mettre en cache l'ensemble des résultats.</p>
<code>-Sql</code>	<code>sql_statement</code>	Facultatif. Entrez une instruction SQL si vous ne voulez pas être en mode interactif.

ListColumnOptions

Répertorie les propriétés des colonnes dans une table virtuelle.

La commande `infacmd sql ListColumnOptions` utilise la syntaxe suivante :

```
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|-sqlds> sql_data_service
<-Table|-t> schema.table
<-Column|-c> column

```

Le tableau suivant décrit les options et les arguments de la commande infacmd sql ListColumnOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
SQLDataService -sqlds	sql_data_service	Requis. Nom du service de données SQL.
-Table -t	schema.table	Requis. Nom de la table. Définissez la table avec la syntaxe suivante : <schema_name>.<table_name>
-Column -c	colonne	Requis. Nom de la colonne.

ListColumnPermissions

Répertorie les autorisations d'utilisateur et de groupe pour une colonne virtuelle.

La syntaxe de la commande infacmd sql ListColumnPermissions est la suivante :

```
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>
```

Le tableau suivant décrit les options et arguments d'infacmd sql ListTablePermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.

Option	Argument	Description
-UserName -un	user_name	<p>Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>
-Password -pd	mot de passe	<p>Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p>
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Durée en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>
SQLDataService -sqlds	sql_data_service	<p>Requis. Nom du service de données SQL.</p> <p>Vous devez préfixer le nom du service de données SQL avec le nom d'application.</p> <p>Utilisez la syntaxe suivante :</p> <pre><nom de l'application>.<nom du service de données SQL></pre>
-Table -t	schema.table	<p>Requis. Nom de la table. Définissez la table avec la syntaxe suivante :</p> <pre><schema_name>.<table_name></pre>

Option	Argument	Description
-Column -c	colonne	Requis. Nom de la colonne à mettre à jour.
-Direct -Effective>	direct effective	Requis. Saisissez soit direct, soit effective. Les autorisations directes sont des autorisations attribuées directement à l'utilisateur ou au groupe. Les autorisations effectives comprennent les autorisations directes et les autorisations héritées.

ListSQLDataServiceOptions

Liste les propriétés d'un service de données SQL qui est déployé vers un service d'intégration de données.

La commande `infacmd sql ListSQLDataServiceOptions` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'`infacmd sql ListSQLDataServiceOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.

Option	Argument	Description
-UserName -un	user_name	<p>Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>
-Password -pd	mot de passe	<p>Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p>
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>
-SQLDataService -sqlds	sql_data_service	<p>Requis. Nom du service de données SQL.</p> <p>Vous devez préfixer le nom du service de données SQL avec le nom d'application.</p> <p>Utilisez la syntaxe suivante :</p> <pre><nom de l'application>.<nom du service de données SQL></pre>

ListSQLDataServicePermissions

Répertorie les autorisations pour un service de données SQL.

La commande infacmd SQL ListSQLDataServicePermissions utilise la syntaxe suivante :

```
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>
```

Le tableau suivant décrit les options et arguments d'infacmd sql ListSQLDataServicePermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
SQLDataService -sqlds	sql_data_service	Requis. Nom du service de données SQL. Vous devez préfixer le nom du service de données SQL avec le nom d'application. Utilisez la syntaxe suivante : <nom de l'application>.<nom du service de données SQL>
-Direct -Effective>	direct effective	Requis. Niveau des autorisations à répertorier. Les autorisations directes sont des autorisations attribuées directement à l'utilisateur ou au groupe. Les autorisations effectives comprennent les autorisations directes et les autorisations héritées.

ListSQLDataServices

Répertorie les services de données SQL d'un service d'intégration de données.

La commande `infacmd sql ListSQLDataServices` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd sql ListSQLDataServices :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Service d'intégration de données dans lequel l'application est déployée.

ListStoredProcedurePermissions

Répertorie les autorisations pour une procédure stockée.

La commande infacmd sql ListStoredProcedurePermissions utilise la syntaxe suivante :

```
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>
```

Le tableau suivant décrit les options et arguments d'infacmd sql ListStoredProcedurePermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
SQLDataService -sqlds	sql_data_service	Requis. Nom du service de données SQL. Vous devez préfixer le nom du service de données SQL avec le nom d'application. Utilisez la syntaxe suivante : <nom de l'application>.<nom du service de données SQL>
StoredProcedure -sp	stored_procedure	Requis. Nom de la procédure stockée.
-Direct -Effective>	direct effective	Requis. Niveau des autorisations à répertorier. Les autorisations directes sont des autorisations attribuées directement à l'utilisateur ou au groupe. Les autorisations effectives comprennent les autorisations directes et les autorisations héritées.

ListTableOptions

Répertorie les propriétés d'une table virtuelle.

La commande infacmd sql ListTableOptions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd sql ListTableOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
SQLDataService -sqlds	sql_data_service	Requis. Nom du service de données SQL. Vous devez préfixer le nom du service de données SQL avec le nom d'application. Utilisez la syntaxe suivante : <nom de l'application>.<nom du service de données SQL>
-Table -t	schema.table	Requis. Nom de la table. Définissez la table avec la syntaxe suivante : <schema_name>.<table_name>

ListTablePermissions

Répertorie les autorisations d'utilisateur et de groupe pour une table virtuelle.

La commande infacmd sql ListTablePermissions utilise la syntaxe suivante :

```
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>
```

Le tableau suivant décrit les options et arguments d'infacmd sql ListTablePermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
SQLDataService -sqlds	sql_data_service	Requis. Nom du service de données SQL. Vous devez préfixer le nom du service de données SQL avec le nom d'application. Utilisez la syntaxe suivante : <nom de l'application>.<nom du service de données SQL>
-Table -t	schema.table	Requis. Nom de la table. Définissez la table avec la syntaxe suivante : <schema_name>.<table_name>
-Direct -Effective>	direct effective	Requis. Saisissez soit direct, soit effective. Les autorisations directes sont des autorisations attribuées directement à l'utilisateur ou au groupe. Les autorisations effectives comprennent les autorisations directes et les autorisations héritées.

PurgeTableCache

Purge le cache de la table virtuelle.

La commande `infacmd sql PurgeTableCache` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd sql PurgeTableCache :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.

Option	Argument	Description
-SQLDataService -sqlds	sql_data_service	Requis. Nom du service de données SQL. Vous devez préfixer -sqlds avec le nom de l'application. Utilisez la syntaxe suivante : <nom de l'application>.<nom du service de données SQL>
-Table -t	table	Requis. Nom du cache de table virtuelle à supprimer.

RefreshTableCache

Actualise un cache de table virtuelle.

La commande infacmd sql RefreshTableCache utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd sql RefreshTableCache :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.
-SQLDataService -sqlds	sql_data_service	Requis. Nom du service de données SQL. Vous devez préfixer -sqlds avec le nom de l'application. Utilisez la syntaxe suivante : <nom de l'application>.<nom du service de données SQL>
-Table -t	table	Requis. Nom du cache de table virtuelle à actualiser.

RenameSQLDataService

Renomme un service de données SQL déployé dans un service d'intégration de données.

La commande infacmd sql RenameSQLDataService utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et arguments d'infacmd sql RenameSQLDataService :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel le service de données SQL est déployé.
-SQLDataService -sqlds	sql_data_service	Requis. Nom du service de données SQL à renommer. Vous devez préfixer le nom du service de données SQL avec le nom d'application. Utilisez la syntaxe suivante : <nom de l'application>.<nom du service de données SQL>
NewName -n	new_name	Requis. Nouveau nom du service de données SQL.

SetColumnPermissions

Refuse à un groupe ou à un utilisateur d'accéder à une colonne dans une requête SQL.

La commande infacmd sql SetColumnPermissions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd sql SetColumnPermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-SQLDataService -sqlds	sql_data_service	Requis. Nom du service de données SQL avec la table virtuelle. Vous devez préfixer le nom du service de données SQL avec le nom d'application. Utilisez la syntaxe suivante : <nom de l'application>.<nom du service de données SQL>
-Table -t	schema.table	Requis. Nom de la table virtuelle. Entrez la table au format suivant : <schema_name>.<table_name>
-Column -c	colonne	Nom de la colonne à mettre à jour.
-GranteeUserName GranteeGroupName -gun -ggn	grantee_user_name grantee_group_name	Requis. Nom d'utilisateur ou nom de groupe pour lequel définir ou refuser des autorisations.
- GranteeSecurityDomain -gsdn	grantee_security_domain	Requis si vous utilisez une authentification LDAP et que vous attribuez des autorisations d'utilisateur. Nom du domaine de sécurité auquel appartient l'utilisateur.
-DeniedPermissions -dp	denied_permissions	Requis. Entrez SQL_Select pour empêcher un utilisateur d'inclure la colonne dans une instruction SELECT.

SetSQLDataServicePermissions

Définit les autorisations données aux groupes ou aux utilisateurs pour un service de données SQL. Vous pouvez également refuser des autorisations.

La commande `infacmd sql SetSQLDataServicePermissions` utilise la syntaxe suivante :

```
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

Le tableau suivant décrit les options et arguments d'infacmd sql SetSQLDataServicePermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel la commande <i>infacmd</i> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-SQLDataService -sqlds	sql_data_service	Requis. Nom du service de données SQL. Vous devez préfixer le nom du service de données SQL avec le nom d'application. Utilisez la syntaxe suivante : <nom de l'application>.<nom du service de données SQL>
-GranteeUserName GranteeGroupName -gun -ggn	grantee_user_name grantee_group_name	Requis. Nom d'utilisateur ou nom de groupe pour lequel définir ou refuser des autorisations.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Requis si vous utilisez une authentification LDAP et que vous attribuez des autorisations d'utilisateur. Nom du domaine de sécurité auquel appartient l'utilisateur.
-AllowedPermissions -ap	allowed_permissions	Requis. Liste des autorisations séparées par des espaces. Entrez l'une des autorisations suivantes : <ul style="list-style-type: none"> - Grant. Les utilisateurs peuvent accorder et retirer des autorisations sur le service de données SQL à l'aide de l'outil Administrator tool ou en utilisant le programme de ligne de commande infacmd. - Execute. Les utilisateurs peuvent exécuter toutes les procédures stockées virtuelles dans le service de données SQL à l'aide d'un outil client JDBC ou ODBC. - SQL_Select. Les utilisateurs peuvent exécuter les instructions SQL SELECT sur les tables virtuelles dans le service de données SQL à l'aide d'un outil client JDBC ou ODBC.
-DeniedPermissions -dp	denied_permissions	Facultatif. Liste des autorisations pour refuser des utilisateurs. Séparez chaque paramètre par une espace. Entrez l'une des autorisations suivantes : <ul style="list-style-type: none"> - EXECUTE. Les utilisateurs ne peuvent pas exécuter de procédure stockée virtuelle dans le service de données SQL. - SQL_SELECT. Les utilisateurs ne peuvent exécuter les instructions SELECT sur aucune table dans le service de données SQL.

SetStoredProcedurePermissions

Définit les autorisations de l'utilisateur et du groupe d'une procédure stockée. Vous pouvez également refuser des autorisations.

La commande infacmd sql SetStoredProcedurePermissions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd sql SetStoredProcedurePermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-SQLDataService -sqlds	sql_data_service	Requis. Nom du service de données SQL avec la procédure stockée. Vous devez préfixer le nom du service de données SQL avec le nom d'application. Utilisez la syntaxe suivante : <nom de l'application>.<nom du service de données SQL>
-StoredProcedure -sp	stored_procedure	Requis. Nom de la procédure stockée.
-GranteeUserName GranteeGroupName -gun -ggn	grantee_user_name grantee_group_name	Requis. Nom d'utilisateur ou nom de groupe pour lequel définir ou refuser des autorisations.

Option	Argument	Description
- GranteeSecurityDomain -gsdn	grantee_security_domain	Requis si vous utilisez une authentification LDAP et que vous attribuez des autorisations d'utilisateur. Nom du domaine de sécurité auquel appartient l'utilisateur.
-AllowedPermissions -ap	list_of_allowed_permissions_separated_by_space	Requis. Liste des autorisations à accepter. Entrez l'un des paramètres suivants séparés par une espace : <ul style="list-style-type: none"> - Grant. Les utilisateurs peuvent accorder et retirer des autorisations sur les objets procédure stockée à l'aide de l'outil Administrator tool ou en utilisant le programme de ligne de commande infacmd - Execute. Les utilisateurs peuvent exécuter des procédures stockées virtuelles dans le service de données SQL via un outil client JDBC ou ODBC.
-DeniedPermissions -dp	denied_permissions	Facultatif. Liste des autorisations pour refuser des utilisateurs. Entrez l'un des paramètres suivants séparés par une espace : <ul style="list-style-type: none"> - GRANT. Les utilisateurs ne peuvent pas accorder ou retirer des autorisations sur les objets procédure stockée. - EXECUTE. Les utilisateurs ne peuvent pas exécuter une procédure stockée dans le service de données SQL.

SetTablePermissions

Définit les autorisations groupe et les autorisations d'utilisateur dans une table virtuelle.

La commande infacmd sql SetTablePermissions utilise la syntaxe suivante :

```
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]

Le tableau suivant décrit les options et arguments d'infacmd sql SetTablePermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>
-SQLDataService -sqlds	sql_data_service	<p>Requis. Nom du service de données SQL avec la table virtuelle.</p> <p>Vous devez préfixer le nom du service de données SQL avec le nom d'application.</p> <p>Utilisez la syntaxe suivante :</p> <p><nom de l'application>.<nom du service de données SQL></p>
-Table -t	schema.table	<p>Requis. Nom de la table virtuelle. Entrez la table au format suivant :</p> <p><schema_name>.<table_name></p>
-GranteeUserName GranteeGroupName -gun -ggn	grantee_user_name grantee_group_name	<p>Requis. Nom d'utilisateur ou nom de groupe pour lequel définir ou refuser des autorisations.</p>
-GranteeSecurityDomain -gsdn	grantee_security_domain	<p>Requis si vous utilisez une authentification LDAP et que vous attribuez des autorisations d'utilisateur. Nom du domaine de sécurité auquel appartient l'utilisateur.</p>

Option	Argument	Description
-AllowedPermissions -ap	list_of_allowed_permissions	Requis. Liste des autorisations à accepter. Entrez les paramètres suivants séparés par une espace : - Grant. Les utilisateurs peuvent accorder et retirer des autorisations sur les objets procédure stockée à l'aide de l'outil Administrator tool ou en utilisant le programme de ligne de commande infacmd. - SQL_Select. Les utilisateurs peuvent exécuter des requêtes SQL sur la table.
-DeniedPermissions -dp	denied_permissions	Facultatif. Liste des autorisations pour refuser des utilisateurs. Entrez les paramètres suivants séparés par une espace : - GRANT. Les utilisateurs ne peuvent pas accorder ou retirer des autorisations sur la table. - SQL_SELECT. Les utilisateurs ne peuvent pas exécuter des requêtes SQL sur la table.
-RLSPredicate -rls	row_level_security_predicate	Facultatif. Répertorie le prédicat de sécurité de niveau ligne à appliquer aux instructions SELECT.

StartSQLDataService

Démarre un service de données SQL.

La commande `infacmd sql StartSQLDataService` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd sql StartSQLDataService :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-SQLDataService -sqlds	sql_data_service	Requis. Nom du service de données SQL. Vous devez préfixer le nom du service de données SQL avec le nom d'application. Utilisez la syntaxe suivante : <nom de l'application>.<nom du service de données SQL>

StopSQLDataService

Arrête l'exécution d'un service de données SQL.

La commande infacmd sql StopSQLDataService utilise la syntaxe suivante :

```
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
```


Le tableau suivant décrit les options et arguments d'infacmd sql StopSQLDataService :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel le service de données SQL est déployé.
-SQLDataService -sqlds	sql_data_service	Requis. Nom du service de données SQL à arrêter. Vous devez préfixer le nom du service de données SQL avec le nom d'application. Utilisez la syntaxe suivante : <nom de l'application>.<nom du service de données SQL>

UpdateColumnOptions

Définit les options de colonnes pour déterminer les actions qui surviennent lorsqu'un utilisateur sélectionne une colonne restreinte dans une requête. Vous pouvez remplacer la valeur par NULL ou par une valeur constante.

La commande `infacmd sql UpdateColumnOptions` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments de la commande `infacmd sql UpdateColumnOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.

Option	Argument	Description
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_se conds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-SQLDataService -sqlds	sql_data_service	Requis. Nom du service de données SQL avec la table virtuelle. Vous devez préfixer le nom du service de données SQL avec le nom d'application. Utilisez la syntaxe suivante : <nom de l'application>.<nom du service de données SQL>
-Table -t	schema.table	Requis. Nom de la table virtuelle. Entrez la table au format suivant : <schema_name>.<table_name>

Option	Argument	Description
-Column -c	colonne	Nom de la colonne.
-Options -o	options	Requis. Entrez chaque option en la séparant par un espace. Pour afficher les options actuelles, exécutez la commande <code>infacmd sql ListColumnOptions</code> .

Options de colonne

Utilisez les options de colonne pour mettre à jour une colonne. Utilisez les options de colonne avec la commande `infacmd sql UpdateColumnOptions`.

Entrez les options de colonne au format suivant :

```
... -o UpdateColumnOptions.option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de colonne :

Options	Description
ColumnOptions.DenyWith	Lorsque vous utilisez le niveau de sécurité de colonne, cette propriété décide de la substitution de la valeur de colonne restreinte ou de l'échec de la requête. Si vous substituez la valeur de colonne, vous pouvez choisir de remplacer la valeur par un NULL ou une valeur constante. Sélectionnez l'une des options suivantes : <ul style="list-style-type: none"> - ERROR. Échec de la requête et renvoi d'une erreur. - NULL. Renvoie les valeurs null pour une colonne restreinte dans chaque ligne. - VALUE. Renvoie une valeur de constante dans la colonne restreinte au niveau de chaque ligne. Configurez la valeur de constante dans l'option <code>InsufficientPermissionValue</code>.
ColumnOptions.InsufficientPermissionValue	Effectue le remplacement de la valeur de la colonne restreinte par une valeur constante. La valeur par défaut est une chaîne vide. Si vous ne configurez pas <code>ColumnOptions.DenyWith</code> , le service d'intégration de données ignore l'option <code>InsufficientPermissionValue</code> .

UpdateSQLDataServiceOptions

Met à jour les propriétés du service de données SQL. Vous devez arrêter le service de données SQL avant de mettre à jour les propriétés.

La commande `infacmd sql UpdateSQLDataServiceOptions` utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et arguments de la commande `infacmd sql UpdateSQLDataServiceOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-SQLDataService -sqlds	sql_data_service	Requis. Nom du service de données SQL. Vous devez préfixer le nom du service de données SQL avec le nom d'application. Utilisez la syntaxe suivante : <nom de l'application>.<nom du service de données SQL>
options -o	options	Requis. Liste des options à mettre à jour. Entrez les options et les valeurs en les séparant par des espaces. Pour afficher les options pour un service de données SQL, exécutez la commande infacmd sql ListSQLDataServiceOptions.

Options du service de données SQL

Utilisez les options du service de données SQL pour mettre à jour un service de données SQL. Utilisez les options du service de données SQL avec la commande infacmd sql UpdateSQLDataServiceOptions.

Entrez les options de service de données SQL dans le format suivant :

```
... -o SQLDataServiceOptions.option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de connexion pour infacmd sql UpdateSQLDataServiceOptions :

Option	Description
SQLDataServiceOptions.startupType	Détermine si le service de données SQL est activé de façon à s'exécuter lors du démarrage de l'application ou lorsque vous démarrez le service de données SQL. Entrez ENABLED pour autoriser l'exécution du service de données SQL. Entrez DISABLED pour empêcher l'exécution du service de données SQL.
SQLDataServiceOptions.traceLevel	Niveau des messages d'erreur écrits dans le journal de session. Spécifiez l'un des niveaux de message suivants : <ul style="list-style-type: none"> - Fatale - Erreur - Informations - Trace - Déboguer
SQLDataServiceOptions.connectionTimeout	Temps d'attente maximal en millisecondes pour l'obtention d'une connexion au service de données SQL. La valeur par défaut est 3 600 000.
SQLDataServiceOptions.requestTimeout	Délai d'attente maximal en millisecondes d'une demande SQL avant d'obtenir la réponse d'un service de données SQL. La valeur par défaut est 3 600 000.
SQLDataServiceOptions.sortOrder	Ordre de tri que le service d'intégration de données utilise pour trier et comparer des données lorsqu'il s'exécute en mode Unicode. Vous pouvez choisir l'ordre de tri selon votre page de code. Lorsque le service d'intégration de données est exécuté en mode ASCII, il ignore la valeur de l'ordre de tri et utilise un ordre de tri binaire. La valeur par défaut est binaire.
SQLDataServiceOptions.maxActiveConnections	Nombre maximal de connexions actives au service de données SQL. La valeur par défaut est 10.
SQLDataServiceOptions.ResultSetCacheExpirationPeriod	Délai en millisecondes pendant lequel le cache de l'ensemble de résultats est utilisable. Si défini sur -1, le cache n'expire jamais. Si défini sur 0, la mise en cache de l'ensemble des résultats est désactivée. Les modifications de la période d'expiration ne s'appliquent pas aux caches existants. Si vous voulez que tous les caches utilisent la même période d'expiration, purgez le cache de l'ensemble des résultats après avoir modifié la période d'expiration. La valeur par défaut est 0.

Option	Description
SQLDataServiceOptions.DTMKeepAliveTime	<p>Nombre de millisecondes pendant lesquelles l'instance DTM demeure ouverte après le traitement de la dernière demande. Les requêtes SQL identiques peuvent réutiliser l'instance ouverte. Utilisez le délai keepalive pour améliorer les performances lorsque le délai requis pour traiter la requête SQL est limité par rapport au délai d'initialisation de l'instance DTM. Si la demande échoue, l'instance DTM prend fin.</p> <p>Doit être un nombre entier. Une valeur entière négative indique que l'intervalle de temps Garder actif DTM pour le service d'intégration de données est utilisé. 0 signifie que le service d'intégration de données ne conserve pas l'instance DTM en mémoire. Valeur par défaut : -1.</p>
SQLDataServiceOptions.optimizeLevel	<p>Niveau d'optimisation que le service d'intégration de données applique à l'objet. Entrez la valeur numérique associée au niveau d'optimisation que vous voulez configurer. Vous pouvez entrer l'une des valeurs numériques suivantes :</p> <ul style="list-style-type: none"> - 0. Le service d'intégration de données n'applique pas d'optimisation. - 1. Le service d'intégration de données applique la méthode d'optimisation de projection précoce. - 2. Le service d'intégration de données applique les méthodes d'optimisation de projection précoce, de sélection précoce, push-into et de prédicat. - 3. Le service d'intégration de données applique les méthodes d'optimisation de projection précoce, de sélection précoce, push-into, de prédicat et de semi-jointure basées sur les coûts.

UpdateTableOptions

Met à jour les propriétés de la table virtuelle. Vous devez arrêter le service de données SQL avant de mettre à jour les propriétés.

La commande infacmd sql UpdateTableOptions utilise la syntaxe suivante :

```
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
```


Le tableau suivant décrit les options et arguments de la commande infacmd sql UpdateTableOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel l'application est déployée.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
SQLDataService -sqlds	sql_data_service	Requis. Nom du service de données SQL. Vous devez préfixer le nom du service de données SQL avec le nom d'application. Utilisez la syntaxe suivante : <nom de l'application>.<nom du service de données SQL>
-Table -t	schema.table	Requis. Nom de la table. Utilisez la syntaxe suivante : <schema_name>.<table_name>
Options -o	options	Requis. Entrez la paire nom-valeur séparée par des espaces.

Options de la table virtuelle

Utilisez les options de la table virtuelle pour configurer la mise en cache d'une table virtuelle. Utilisez les options de la table virtuelle avec la commande `infacmd sql UpdateTableOptions`.

Entrez les options de table virtuelle au format suivant :

```
... -o option_type.option_name=value ...
```

Pour entrer plusieurs options, séparez-les par un espace. Pour entrer une valeur contenant un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options de table virtuelle :

Option	Description
VirtualTableOptions.CachingEnabled	Mise en cache de la table virtuelle dans la base de données du cache d'objet de données. True ou False. La valeur par défaut est True.
VirtualTableOptions.CacheRefreshPeriod	Nombre de minutes entre les actualisations du cache. La valeur par défaut est zéro.
VirtualTableOptions.CacheTableName	Nom de la table gérée par l'utilisateur à partir de laquelle le service d'intégration de données accède au cache de la table virtuelle. Une table de cache gérée par l'utilisateur est une table de la base de données du cache d'objet de données que vous créez, remplissez et actualisez manuellement si nécessaire. Si vous spécifiez un nom de table de cache, le gestionnaire de cache d'objet de données ne gère pas le cache de l'objet et ignore la période d'actualisation du cache. Si vous ne spécifiez pas de nom de table de cache, le gestionnaire de cache d'objet de données gère le cache de l'objet.

CHAPITRE 36

Référence de commande infacmd tdm

Le programme *infacmd tdm* administre le service Test Data Manager.

Vous pouvez créer le service, lui ajouter un contenu, l'activer et le désactiver à l'aide des commandes *infacmd tdm*.

CreateService

Crée un service Test Data Manager dans un domaine.

La commande *infacmd tdm CreateService* utilise la syntaxe suivante :

```
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

<-PCRSServiceName|-pcrs> power_center_repo_service
<-PCISServiceName|-pcis> power_center_int_service

<-MRSServiceName|-mrs> model_repo_service
<-MRSUserName|-rsun> model_repo_service_username
<-MRSPassword|-rspd> model_repo_service_password
```

```

[<-MRSSecurityDomain|-rsdn> model_repo_security_domain]

<-AnalystService|-at> analyst_service
<-EnableProfiling|-ep> enable_profiling
<-TDWServiceName|-tdw> test_data_warehouse_service

<-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
<-DBConnString|-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]

```

Le tableau suivant décrit les options et arguments d'infacmd tdm CreateService :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service Test Data Manager. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Les caractères doivent être compatibles avec la page de code du référentiel associé. Le nom ne peut pas dépasser 230 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire. La valeur par défaut est 180 secondes.
-NodeName -nn	node_name	Requis. Nom du nœud sur lequel le service s'exécutera.
-LicenseName -ln	license_name	Requis. Nom de la licence. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Le nom ne peut pas dépasser 79 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "
-PCRSServicename -pcrs	power_center_repo_service	Nom du service de référentiel PowerCenter auquel TDM se connecte.
-PCISServicename -pcis	power_center_int_service	Nom du service d'intégration PowerCenter auquel TDM se connecte.
-MRSServiceName -mrs	model_repo_service	Nom du service de référentiel modèle auquel TDM se connecte.
-MRSUserName -rsun	model_repo_service_username	Requis. Nom d'utilisateur pour la connexion au référentiel modèle.

Option	Argument	Description
-MRSPassword -rspd	model_repo_service_password	Requis. Mot de passe du nom d'utilisateur pour la connexion au référentiel modèle. Le mot de passe est sensible à la casse.
-AnalystService -at	analyst_service	Facultatif. Nom du service Analyst que TDM utilise pour la liaison d'actifs. Requis si vous utilisez la fonctionnalité de liaison d'actifs pour lier les objets TDM globaux aux objets Business Glossary.
-MRSSecurityDomain -rsdn	model_repo_security_domain	Requis si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.
-EnableProfiling -ep	enable_profiling	Indique les paramètres de découverte de données. Définissez sur True pour activer la découverte de données. Définissez sur False pour désactiver la découverte de données.
-TDWServiceName tdw	test_data_warehouse_service	Facultatif. Requis si vous créez un Test Data Warehouse. Nom du service Test Data Warehouse que TDM utilise pour gérer Test Data Warehouse.
-DISServiceName -dis	data_integration_service	Nom du service d'intégration de données auquel TDM se connecte.
-db_type -dt	database_type	Type de la base de données du référentiel TDM. Les valeurs sont Oracle, SQL Server, DB2 ou Personnalisé.
-DBUsername -du	db_user	Requis. Compte de la base de données du référentiel. Utilisez le client de base de données pour configurer ce compte.
-DBPassword -dp	db_password	Requis. Mot de passe de la base de données du référentiel pour l'utilisateur de la base de données.

Option	Argument	Description
-DBUrl -dl	db_url	<p>Requis. Chaîne de connexion JDBC à la base de données pour le référentiel TDM. Utilisez l'une des syntaxes suivantes :</p> <p>Oracle :</p> <pre>jdbc:informatica:oracle: // <machineName>:<PortNo>;ServiceName= <DBName>; MaxPooledStatements=20; CatalogOptions=0; EnableServerResultCache=true</pre> <p>DB2 :</p> <pre>jdbc:informatica:db2: //<host>:<port>; DatabaseName=<dbname>; BatchPerformanceWorkaround=true;Dynamic Sections=1000</pre> <p>SQLServer :</p> <pre>jdbc:informatica:sqlserver: // <host>:<port>; DatabaseName=<dbname>; SnapshotSerializable=true</pre>
-DBConnString -dc	db_conn_string	Chaîne de connexion native pour la base de données du référentiel TDM. Le service utilise la chaîne de connexion pour créer un objet de connexion aux référentiels Test Data Manager et PowerCenter ou au référentiel modèle.
-DbSchema -ds	db_schema	Facultatif. Nom de schéma pour une base de données Microsoft SQL Server.
-DbTablespace -db	db_tablespace	<p>Requis uniquement pour une base de données DB2. Lorsque vous configurez un nom d'espace de table, le service Test Data Manager crée toutes les tables du référentiel dans le même espace de table. Le nom de l'espace de table ne doit pas contenir d'espaces.</p> <p>L'espace de table doit être défini dans un seul nœud et la taille de page doit être de 32 Ko. Dans une base de données multipartition, vous devez sélectionner cette option. Dans une base de données à partition unique, si vous ne sélectionnez pas cette option, le programme d'installation crée les tables dans l'espace de table par défaut.</p>
-HttpPort	http_port	Requis. Numéro de port pour le service.
-HttpsPort	https_port	Facultatif. Numéro de port pour sécuriser la connexion à l'outil Administrator tool. Définissez ce numéro de port si vous souhaitez configurer HTTPS pour un nœud.
-KeystoreFile -kf	keystore_file_location]	Facultatif. Le fichier keystore contenant les clés et les certificats est requis en cas d'utilisation du protocole de sécurité SSL avec PowerCenter.

Option	Argument	Description
-KeystorePassword -kp	keystore_password	Facultatif. Si le protocole TLS est activé, vous devez spécifier un mot de passe.
-SSLProtocol -pt	Protocole SSL	Facultatif. Protocole Secure Sockets Layer à utiliser. Modifiable si vous activez TLS (Transport Layer Security).
-jvmParams -jp	jvmParameters	<p>Paramètres JVM à définir :</p> <ul style="list-style-type: none"> - Taille du tas mémoire allouée à Test Data Manager. - Délai au bout duquel les connexions de base de données sont renouvelées si l'interface utilisateur de TDM reste inactive. Requis si vous avez modifié les paramètres de configuration de la base de données en indiquant des valeurs inférieures à celles par défaut de TDM. Modifiez les valeurs dans TDM de façon qu'elles soient inférieures à celles de la base de données. <p>Inclure les paramètres JVM dans des guillemets simples, puis dans des guillemets doubles. Par exemple, 'value', puis "value".</p> <p>L'option -Xms est sensible à la casse. Par exemple :</p> <p>""- Xms512m - Xmx1024m - XX:MaxPermSize=512m""</p> <ul style="list-style-type: none"> - IDLE_TIME. -DIDLE_TIME=<secondes>. La valeur par défaut est 300 secondes. - CONNECT_TIME. -DCONNECT_TIME=<secondes>. La valeur par défaut est 5000 secondes.
-connPoolSize -cp	conn_pool_size	Facultatif. Nombre maximal d'instances de connexions inactives conservées par un pool pour une connexion de base de données avant que la durée maximale d'inactivité ne soit atteinte. Définissez cette valeur pour qu'elle soit supérieure au nombre minimal d'instances de connexions inactives. La valeur par défaut est 15.
-jmxPort	jmx_port	Numéro de port pour les connexions JMX/RMI à TDM. La valeur par défaut est 6675.
-shutdownPort	shutdown_port	Numéro de port qui contrôle l'arrêt de TDM.
-hadoopDistDir -hdd	Répertoire de distribution Hadoop	Répertoire de distribution Hadoop sur le nœud du service Test Data Manager.

Option	Argument	Description
-hadoopKerbSPN -hks	Nom du principal du service Hadoop Kerberos	Nom de principal du service (SPN) d'intégration de données permettant de se connecter à une grappe Hadoop qui utilise l'authentification Kerberos. Non requis lorsque vous exécutez la distribution MapR Hadoop. Requis pour d'autres distributions Hadoop.
-hadoopKerbKeytab -hkt	Keytab Hadoop Kerberos	Chemin du fichier Keytab Kerberos sur la machine sur laquelle le service d'intégration de données s'exécute. Non requis lorsque vous exécutez la distribution MapR Hadoop. Requis pour d'autres distributions Hadoop.

CreateContents

Crée le contenu pour le référentiel Test Data Manager.

La commande `infacmd tdm CreateContents` utilise la syntaxe suivante :

```
<-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]
```

Le tableau suivant décrit les options et arguments d'infacmd tdm CreateContents :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Le nom du service Test Data Manager.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

EnableService

Active le service Test Data Manager.

La commande infacmd tdm EnableService utilise la syntaxe suivante :

```
<-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]
```

Le tableau suivant décrit les options et arguments d'infacmd tdm EnableService :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service sur lequel exécuter la commande. Pour entrer un nom contenant une espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

DisableService

Désactive le service Test Data Manager. Lorsque vous désactivez le service Test Data Manager, tous les processus du service s'arrêtent.

La commande infacmd tdm DisableService utilise la syntaxe suivante :

```
<-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
```

Le tableau suivant décrit les options et arguments d'infacmd tdm DisableService :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service sur lequel exécuter la commande. Pour entrer un nom contenant une espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_se conds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Si vous omettez cette option, infacmd utilise la valeur de délai d'expiration spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-DisableMode -dm	disable_mode	Obligatoire. Définit le mode désactivation du service : <ul style="list-style-type: none"> - Terminer. Désactive le service lorsque tous les processus de service sont arrêtés. - Abandonner. Interrompt immédiatement tous les processus, puis désactive le service. - Arrêter. Interrompt tous les flux de travail en cours d'exécution, puis désactive le service.

CHAPITRE 37

Référence de commande infacmd tools

Ce chapitre comprend les rubriques suivantes :

- [deployApplication, 1172](#)
- [exportObjects, 1174](#)
- [exportResources, 1177](#)
- [importObjects, 1179](#)
- [patchApplication, 1185](#)

deployApplication

Déploie une application dans un fichier .iar.

Déployez une application dans un fichier lorsqu'elle contient un grand nombre d'objets. Après avoir exécuté la commande `infacmd tools deployApplication`, exécutez la commande `infacmd dis deployApplication` pour déployer l'application dans un service d'intégration de données.

La syntaxe de la commande `infacmd tools deployApplication` est la suivante :

```
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
```


Le tableau suivant décrit les options et les arguments de la commande `infacmd tools deployApplication` :

Option	Argument	Description
-DomainName -dn	Nom de domaine	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	Nom d'utilisateur	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	Mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	Domaine de sécurité	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
- RepositoryService -rs	Nom du service de référentiel modèle	Requis. Nom du service de référentiel modèle.
- OutputDirectory -od	Répertoire de sortie	Obligatoire. Répertoire dans lequel vous souhaitez écrire le fichier .iar.
- ApplicationPath -ap	Chemin de l'application	Obligatoire. Chemin de l'application, qui commence par le nom du projet et les noms des dossiers, suivis du nom de l'application. Séparez le nom du projet, les noms des dossiers et le nom de l'application par une barre oblique (/). Par exemple, « Project/Folder1/Folder2/Application ».

exportObjects

Exporte les objets d'un projet présent dans le référentiel modèle vers un fichier XML.

Si vous ne voulez pas exporter tous les objets dans le projet, utilisez le fichier de contrôle d'exportation `infacmd` pour filtrer les objets du référentiel modèle que vous souhaitez exporter.

Si le projet exporté contient des tables de référence, vous devez exécuter la commande depuis le répertoire d'installation des services Informatica. La commande exporte les métadonnées de la table de référence du référentiel modèle au fichier XML. La commande exporte les données de la table de référence vers un fichier ZIP. Lorsque vous exécutez la commande, spécifiez le chemin et le nom de fichier des fichiers XML et ZIP à créer.

La commande n'exporte pas les dossiers vides.

Si la commande échoue et renvoie une erreur de mémoire Java, augmentez la mémoire système disponible pour `infacmd`. Pour augmenter la mémoire système, définissez la valeur `-Xmx` dans la variable d'environnement `ICMD_JAVA_OPTS`.

La syntaxe de la commande `infacmd tools exportObjects` est la suivante :

```
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>]
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd tools exportObjects` :

Option	Argument	Description
-DomainName -dn	Nom de domaine	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	Nom d'utilisateur	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	Mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	Domaine de sécurité	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ProjectName -pn	Nom de projet	Obligatoire. Nom du projet d'où vous exportez les objets.
-RepositoryService -rs	Nom du service de référentiel modèle	Requis. Nom du service de référentiel modèle.

Option	Argument	Description
-ExportFilePath -fp	Chemin d'accès du fichier à exporter vers	Obligatoire. Chemin et nom du fichier XML du fichier d'exportation à créer. Vous pouvez spécifier un chemin d'accès absolu ou relatif pour le nom du fichier. Utilisez un nom facilement identifiable pour le fichier. Par exemple, utilisez la convention de dénomination suggérée suivante: <code>exp_<project_name></code> Remarque: La commande ajoute l'extension de fichier .xml au fichier de sortie.
-OverwriteExportFile -ow	Définir sur « Vrai » pour écraser le fichier d'exportation s'il existe.	Facultatif. Défini sur « Vrai » pour écraser un fichier d'exportation existant. Si un fichier d'exportation existe et que cette option est définie sur « Faux », l'exportation échoue. La valeur par défaut est false.
-ControlFilePath -cp	Chemin d'accès du fichier de contrôle d'exportation	Facultatif. Chemin et nom du fichier de contrôle d'exportation qui filtre les objets exportés. Vous pouvez spécifier un chemin d'accès absolu ou relatif pour le nom de fichier.
-OtherOptions -oo	-	Obligatoire si le projet exporté contient des tables de référence. Autres options pour exporter les données de table de référence vers un fichier ZIP. Entrez les options en utilisant le format suivant : <code>rtm:<option_name>=<value>,<option_name>=<value></code> Les noms d'option requis incluent : <ul style="list-style-type: none"> - <code>disName</code>. Nom du service d'intégration de données. - <code>codePage</code>. Page de code des données de référence. - <code>refDataFile</code>. Chemin et nom du fichier zip où vous voulez exporter les données de la table de référence. Par exemple : <code>rtm:disName=ds,codePage=UTF-8,refDataFile=/folder1/data.zip</code>

Option	Argument	Description
-DomainName -dn	Nom de domaine	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	Nom d'utilisateur	Requis. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Password -pd	Mot de passe	Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.
-SecurityDomain -sdn	Domaine de sécurité	Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.

Option	Argument	Description
-ProjectName -pn	Nom de projet	Obligatoire. Nom du projet d'où vous exportez les objets.
-RepositoryService -rs	Nom du service de référentiel modèle	Requis. Nom du service de référentiel modèle.
-ExportFilePath -fp	Chemin d'accès du fichier à exporter vers	Obligatoire. Chemin et nom du fichier XML du fichier d'exportation à créer. Vous pouvez spécifier un chemin d'accès absolu ou relatif pour le nom du fichier. Utilisez un nom facilement identifiable pour le fichier. Par exemple, utilisez la convention de dénomination suggérée suivante: exp_<project_name>.xml
-OverwriteExportFile -ow	Définir sur « Vrai » pour écraser le fichier d'exportation s'il existe.	Facultatif. Défini sur « Vrai » pour écraser un fichier d'exportation existant. Si un fichier d'exportation existe et que cette option est définie sur « Faux », l'exportation échoue. La valeur par défaut est false.
-ControlFilePath -cp	Chemin d'accès du fichier de contrôle d'exportation	Facultatif. Chemin et nom du fichier de contrôle d'exportation qui filtre les objets exportés. Vous pouvez spécifier un chemin d'accès absolu ou relatif pour le nom de fichier.

exportResources

Exporte des objets fiche d'évaluation et des informations de lignage d'un projet ou d'un dossier vers un fichier XML que vous utilisez dans le gestionnaire de métadonnées.

Si vous ne voulez pas exporter tous les objets du projet, utilisez le fichier de contrôle d'exportation infacmd pour filtrer les objets que vous souhaitez exporter. La commande n'exporte pas les dossiers vides.

Si la commande échoue et renvoie une erreur de mémoire Java, augmentez la mémoire système disponible pour infacmd. Pour augmenter la mémoire système, définissez la valeur `-Xmx` dans la variable d'environnement `ICMD_JAVA_OPTS`.

La syntaxe de la commande `infacmd tools exportResources` est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd tools exportResources` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ProjectName -pn	project_name	Requis. Nom du projet d'où vous exportez les objets.
-RepositoryService -rs	model_repository_service_name	Requis. Nom du service de référentiel modèle.

Option	Argument	Description
-ExportFilePath -fp	export_file_path	Obligatoire. Chemin d'accès et nom de fichier XML du fichier d'exportation que le programme de ligne de commande crée lorsque vous exécutez la commande. Vous pouvez spécifier un chemin d'accès absolu ou relatif au nom de fichier. Utilisez un nom facile à retenir pour le fichier. Par exemple, utilisez la convention de dénomination suggérée suivante : exp_<project_name>.xml
-OverwriteExportFile -ow	overwrite_export_file	Facultatif. Définissez cette option sur true pour écraser un fichier d'exportation existant. Si un fichier d'exportation existe et que vous définissez cette option sur false, l'exportation échoue. La valeur par défaut est false.
-ControlFilePath -cp	control_file_path	Facultatif. Le chemin d'accès et le nom du fichier de contrôle d'exportation qui filtre les objets exportés par le programme de ligne de commande. Vous pouvez spécifier un chemin d'accès absolu ou relatif au nom de fichier.

importObjects

Importe les objets d'un fichier XML à un projet existant dans le référentiel modèle.

Si vous ne voulez pas importer tous les objets dans le fichier, utilisez le fichier de contrôle d'exportation infacmd pour filtrer les objets du référentiel modèle que vous souhaitez importer.

Si le fichier importé contient des tables de référence, vous devez exécuter la commande depuis le répertoire d'installation des services Informatica. La commande importe les métadonnées de la table de référence du fichier XML au référentiel modèle. La commande importe les données de la table de référence depuis un fichier ZIP. Lorsque vous exécutez la commande, spécifiez le chemin et le nom de fichier des fichiers XML et ZIP à importer.

Si la commande échoue et renvoie une erreur de mémoire Java, augmentez la mémoire système disponible pour infacmd. Pour augmenter la mémoire système, définissez la valeur -Xmx dans la variable d'environnement ICMD_JAVA_OPTS.

La syntaxe de la commande infacmd tools importObjects est la suivante :

```
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>]

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.]

Le tableau suivant décrit les options et les arguments de la commande `infacmd tools importObjects` :

Option	Argument	Description
-DomainName -dn	Nom de domaine	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	Nom d'utilisateur	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	Mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	Domaine de sécurité	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-TargetProject -tp	Nom du projet cible <ignored if control file is specified>	Facultatif. Nom du projet dans lequel vous voulez importer les objets. Le projet doit exister dans le référentiel avant d'importer les objets. L'option est ignorée si vous utilisez un fichier de contrôle d'importation.
-RepositoryService -rs	Nom du service de référentiel modèle	Requis. Nom du service de référentiel modèle.
-ImportFilePath -fp	import_file_path	Requis. Chemin et nom du fichier XML à partir duquel importer les objets. Vous pouvez spécifier un chemin absolu ou relatif pour le nom de fichier.
-SourceProject -sp	Nom du projet source dans le fichier d'importation <ignored if control file is specified>	Facultatif. Nom du projet source dans le fichier à importer. L'option est ignorée si vous utilisez un fichier de contrôle d'importation.
-TargetFolder -tf	Dossier cible à importer dans <omit for root, ignored if control file is specified>	Facultatif. Dossier cible dans lequel vous voulez importer les objets. Si vous ne spécifiez pas de dossier cible, les objets sont importés dans le projet cible. Le dossier doit être créé dans le référentiel avant d'importer les objets. L'option est ignorée si vous utilisez un fichier de contrôle d'importation.
-SkipCRC -sc	Si l'option est True, le contrôle CRC est ignoré sur le fichier importé.	Indique s'il faut ignorer le contrôle de redondance cyclique (CRC) qui détecte si le fichier à importer a été modifié. Définissez sur True pour ignorer le contrôle. La valeur par défaut est False.
-ConflictResolution -cr	Type de résolution spécifié	Facultatif. Stratégie de résolution de conflit. Vous pouvez spécifier l'une des options suivantes pour tous les objets importés : <ul style="list-style-type: none"> - renommer - remplacer - réutiliser - aucun L'option est ignorée si vous utilisez un fichier de contrôle d'importation. Si la stratégie de résolution de conflit est définie sur Aucun et qu'un conflit se produit, l'importation échoue. La valeur par défaut est Aucun.
-ControlFilePath -cp	Chemin du fichier de contrôle d'importation	Facultatif. Chemin et nom du fichier de contrôle d'importation qui filtre les objets importés. Vous pouvez spécifier un chemin absolu ou relatif.

Option	Argument	Description
-SkipCnxValidation -scv	Définissez sur True pour ignorer la validation de connexion.	<p>Facultatif. Indique s'il faut ignorer la validation de connexion pendant l'importation. Par défaut, le processus d'importation vérifie que les connexions utilisées par les objets importés existent dans le référentiel cible. L'importation échoue s'il n'y a aucune connexion.</p> <p>Pour ignorer la validation de connexion cible et continuer l'importation, définissez cette option sur True. Si les objets importés utilisent des connexions qui n'existent pas dans le référentiel cible, le processus d'importation importe les objets dont la connexion est « Non spécifiée ». Utilisez l'outil Developer tool pour sélectionner la connexion à la fin du processus d'importation.</p> <p>La valeur par défaut est False.</p> <p>Remarque: Si un fichier de contrôle d'importation spécifie une connexion source qui n'existe pas dans le fichier que vous importez, le processus d'importation échoue, indépendamment de la valeur de cette option. Pour corriger cette erreur, vérifiez que l'élément de rétablissement de la connexion qui se trouve dans le fichier de contrôle d'importation comprend des connexions source qui existent dans le fichier que vous importez.</p>
-OtherOptions -oo	-	<p>Requis si le fichier d'importation contient des tables de référence. Options supplémentaires permettant d'importer les données de la table de référence depuis un fichier ZIP. Entrez les options en utilisant le format suivant :</p> <pre>rtm:<option_name>=<value>,<option_name>=<value></pre> <p>Les noms d'option requis incluent :</p> <ul style="list-style-type: none"> - disName. Nom du service d'intégration de données. - codePage. Page de code des données de référence. - refDataFile. Chemin et nom du fichier zip d'où vous voulez importer les données de la table de référence. <p>Par exemple :</p> <pre>rtm:disName=ds,codePage=UTF-8,refDataFile=/folder1/data.zip</pre>

Option	Argument	Description
-DomainName -dn	Nom de domaine	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez

Option	Argument	Description
		un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	Nom d'utilisateur	Requis. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.
-Password -pd	Mot de passe	Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.
-SecurityDomain -sdn	Domaine de sécurité	Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.
-TargetProject -tp	Nom du projet cible <ignored if control file is specified>	Facultatif. Nom du projet dans lequel vous voulez importer les objets. Le projet doit exister dans le référentiel avant d'importer les objets. L'option est ignorée si vous utilisez un fichier de contrôle d'importation.
-RepositoryService -rs	Nom du service de référentiel modèle	Requis. Nom du service de référentiel modèle.
-ImportFilePath -fp	import_file_path	Requis. Chemin et nom du fichier XML à partir duquel importer les objets. Vous pouvez spécifier un chemin absolu ou relatif pour le nom de fichier.
-SourceProject -sp	Nom du projet source dans le fichier d'importation <ignored if control file is specified>	Facultatif. Nom du projet source dans le fichier à importer. L'option est ignorée si vous utilisez un fichier de contrôle d'importation.
-TargetFolder -tf	Dossier cible à importer dans <omit for root, ignored if control file is specified>	Facultatif. Dossier cible dans lequel vous voulez importer les objets. Si vous ne spécifiez pas de dossier cible, les objets sont importés dans le projet cible. Le dossier doit être créé dans le référentiel avant d'importer les objets. L'option est ignorée si vous utilisez un fichier de contrôle d'importation.
-SkipCRC -sc	Si l'option est True, le contrôle CRC est ignoré sur le fichier importé.	Indique s'il faut ignorer le contrôle de redondance cyclique (CRC) qui détecte si le fichier à importer a été modifié. Définissez sur True pour ignorer le contrôle. La valeur par défaut est False.

Option	Argument	Description
-ConflictResolution -cr	Type de résolution spécifié	Facultatif. Stratégie de résolution de conflit. Vous pouvez spécifier l'une des options suivantes pour tous les objets importés : <ul style="list-style-type: none"> - renommer - remplacer - réutiliser - aucun L'option est ignorée si vous utilisez un fichier de contrôle d'importation. Si la stratégie de résolution de conflit est définie sur Aucun et qu'un conflit se produit, l'importation échoue. La valeur par défaut est Aucun.
-ControlFilePath -cp	Chemin du fichier de contrôle d'importation	Facultatif. Chemin et nom du fichier de contrôle d'importation qui filtre les objets importés. Vous pouvez spécifier un chemin absolu ou relatif.
-SkipCnxValidation -scv	Définissez sur True pour ignorer la validation de connexion.	Facultatif. Indique s'il faut ignorer la validation de connexion pendant l'importation. Par défaut, le processus d'importation vérifie que les connexions utilisées par les objets importés existent dans le référentiel cible. L'importation échoue s'il n'y a aucune connexion. <p>Pour ignorer la validation de connexion cible et continuer l'importation, définissez cette option sur True. Si les objets importés utilisent des connexions qui n'existent pas dans le référentiel cible, le processus d'importation importe les objets dont la connexion est « Non spécifiée ». Utilisez l'outil Developer tool pour sélectionner la connexion à la fin du processus d'importation.</p> <p>La valeur par défaut est False.</p> <p>Remarque: Si un fichier de contrôle d'importation spécifie une connexion source qui n'existe pas dans le fichier que vous importez, le processus d'importation échoue, indépendamment de la valeur de cette option. Pour corriger cette erreur, vérifiez que l'élément de rétablissement de la connexion qui se trouve dans le fichier de contrôle d'importation comprend des connexions source qui existent dans le fichier que vous importez.</p>

patchApplication

Déploye un correctif d'application à l'aide d'un fichier .piar dans un service d'intégration de données. Le service d'intégration de données applique le correctif à l'application incrémentielle correspondante. L'application incrémentielle doit être déployée sur le même service d'intégration de données où vous voulez déployer le correctif.

Si vous avez créé le correctif en fonction d'une version précédente de l'application incrémentielle, le correctif peut ne pas être valide. Un correctif n'est pas valide si les objets d'application du correctif ont été mis à jour par d'autres correctifs de l'application, car le correctif à déployer a été créé. Pour continuer, vous pouvez forcer le service d'intégration de données à appliquer le correctif.

Vous pouvez également choisir de conserver ou d'ignorer les informations d'état. Les informations d'état font référence aux propriétés du mappage et aux propriétés d'objets d'exécution tels que les sorties de mappage ou la transformation Générateur de séquence.

Pour plus de détails sur les informations d'état, consultez le chapitre « Déploiement d'applications » du *Guide de l'outil Informatica Developer tool*.

Remarque: Si vous déployez une version précédente d'un correctif, le service d'intégration de données ne restaure pas l'application incrémentielle au moment où le correctif a été créé. Le service d'intégration de données met à jour l'application en fonction des objets d'application dans le correctif.

La syntaxe de la commande `infacmd tools patchApplication` est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd tools patchApplication` :

Option	Argument	Description
-DomainName -dn	Nom de domaine	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	Nom d'utilisateur	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	Mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	Domaine de sécurité	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-DataIntegrationService -dis	Nom du service d'intégration de données	Obligatoire. Nom du service d'intégration de données dans lequel l'application incrémentielle est déployée.
-FilePath -fp	Chemin d'accès au fichier de correctif	Obligatoire. Chemin et nom de fichier .piar du correctif à déployer. Vous pouvez spécifier un chemin d'accès absolu ou relatif au nom de fichier.
-force -f	True False	Facultatif. Utilisez <code>true</code> pour ignorer la validité du correctif et forcer le service d'intégration de données à appliquer le correctif à l'application. La valeur par défaut est <code>false</code> .
-RetainStateInformation -rsi	True False	<p>Facultatif. Indique s'il convient de conserver ou d'ignorer les informations d'état.</p> <p>Remarque: Cette option remplace les paramètres indiquant de conserver ou d'ignorer les informations d'état dans le fichier d'archive de correctif d'application.</p>

CHAPITRE 38

Référence de la commande infacmd wfs

Ce chapitre comprend les rubriques suivantes :

- [abortWorkflow, 1188](#)
- [bulkComplete, 1190](#)
- [cancelWorkflow, 1192](#)
- [completeTask, 1194](#)
- [createTables, 1196](#)
- [delegateTask, 1198](#)
- [dropTables, 1200](#)
- [listActiveWorkflowInstances, 1201](#)
- [listMappingPersistedOutputs, 1203](#)
- [listTasks, 1205](#)
- [listWorkflowParams, 1208](#)
- [listWorkflows, 1211](#)
- [pruneOldInstances, 1212](#)
- [recoverWorkflow, 1214](#)
- [releaseTask, 1216](#)
- [setMappingPersistedOutputs, 1218](#)
- [startTask, 1221](#)
- [startWorkflow, 1222](#)
- [upgradeWorkflowParameterFile, 1224](#)

abortWorkflow

Abandonne une instance de flux de travail en cours d'exécution.

Si une tâche d'assignation ou une passerelle exclusive sont en cours d'exécution, le service d'intégration de données termine la tâche ou la passerelle. Après abandon ou achèvement de la tâche, le service abandonne l'instance de flux de travail. Le service ne démarre l'exécution d'aucun des objets de flux de travail suivants.

La commande `infacmd wfs abortWorkflow` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande `infacmd wfs abortWorkflow` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données exécutant l'instance de flux de travail.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-InstanceId -iid	ID de l'instance du flux de travail à abandonner	Requis. ID de l'instance du flux de travail à abandonner. Vous pouvez lire l'ID d'instance de flux de travail à partir des propriétés du flux de travail de l'onglet Surveillance de l'outil Administrator tool. Vous pouvez également exécuter la commande <code>infacmd wfs ListActiveWorkflowInstances</code> pour trouver l'ID d'instance de flux de travail.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

bulkComplete

Arrête toutes les opérations d'une tâche humaine dans un flux de travail que vous spécifiez et transmet les enregistrements que la tâche identifie à l'étape suivante du flux de travail. La commande bulkComplete met à jour le statut des étapes dans les tâches humaines pour indiquer que les étapes sont terminées. La commande ne modifie pas ni ne met à jour le statut des enregistrements identifiés par la tâche.

La commande bulkComplete utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd wfs bulkComplete` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui exécute l'instance de flux de travail.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
InstanceID -iid	Instance_ID	Requis. Identifiant unique du flux de travail qui exécute la tâche humaine que vous voulez terminer. Vous pouvez lire l'ID d'instance de flux de travail à partir des propriétés du flux de travail de l'onglet Surveillance de l'outil Administrator tool. Vous pouvez également exécuter la commande <code>infacmd wfs ListActiveWorkflowInstances</code> pour trouver l'ID d'instance de flux de travail.
StepName -sid	Step_name	Requis. Nom de la tâche humaine que le flux de travail utilise pour créer les instances de tâche humaine.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

cancelWorkflow

Annule une instance de flux de travail en cours d'exécution. Lorsque vous annulez une instance de flux de travail, le service d'intégration de données termine le traitement des tâches en cours d'exécution, puis arrête le traitement de l'instance de flux de travail. Le service ne démarre l'exécution d'aucun des objets suivants.

La commande `infacmd wfs cancelWorkflow` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande `infacmd wfs cancelWorkflow` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données exécutant l'instance de flux de travail.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Argument	Description
-InstanceID -iid	instance_ID	Requis. ID de l'instance du flux de travail à annuler. Vous pouvez lire l'ID d'instance de flux de travail à partir des propriétés du flux de travail de l'onglet Surveillance de l'outil Administrator tool. Vous pouvez également exécuter la commande <code>infacmd wfs ListActiveWorkflowInstances</code> pour trouver l'ID d'instance de flux de travail.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option <code>-re</code> ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option <code>-re</code> est prioritaire.

completeTask

Exécute une instance de tâche humaine que vous spécifiez.

Une instance de tâche humaine est un ensemble d'enregistrements qu'un flux de travail attribue à un utilisateur ou à un groupe pour analyse dans Informatica Analyst. La commande `completeTask` met à jour le statut de l'instance de tâche à Terminé et transmet les enregistrements de cette dernière à une autre étape du flux de travail. Par exemple, vous pouvez configurer la commande de sorte à envoyer les enregistrements à une autre instance de tâche pour révision.

Chaque instance de tâche humaine possède un ID d'instance de tâche unique. Lorsque vous exécutez `infacmd wfs completeTask`, vous devez entrer une valeur d'ID pour identifier l'instance de tâche à terminer.

Pour trouver l'ID de l'instance de tâche, procédez de l'une des manières suivantes :

- Connectez-vous à Informatica Analyst et lisez l'ID de l'instance de tâche dans l'outil Monitoring tool.
- Exécutez la commande `infacmd wfs listTasks`.
- Demandez à l'administrateur d'entreprise ou à l'utilisateur propriétaire de l'instance de tâche.
L'administrateur d'entreprise ou l'utilisateur peut lire l'ID de l'instance de tâche dans Informatica Analyst.

La commande `infacmd wfs completeTask` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande `infacmd wfs completeTask` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui exécute l'instance de flux de travail.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-TaskID -tid	task_id	Requis. Identifiant unique de l'instance de tâche humaine.
-NextTask -to	next_task	Requis. Nom de l'étape dans le flux de travail auquel la commande transmet les enregistrements de l'instance de tâche. La configuration de tâche humaine dans le flux de travail détermine les étapes auxquelles les enregistrements de l'instance de tâche peuvent être transmises.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

createTables

Crée les tables de base de données qui stockent les métadonnées d'exécution du flux de travail. La commande crée des tables vides. Identifiez le service qui exécute les flux de travail lorsque vous exécutez la commande.

Avant de créer les tables de base de données, vérifiez les options suivantes sur le service d'intégration de données qui exécute les flux de travail :

- Le module Service d'orchestration du flux de travail est actif sur le service d'intégration de données.
- Les propriétés du service d'orchestration du flux de travail identifient la connexion de la base de données qui stocke les métadonnées du flux de travail.

La commande createTables utilise la syntaxe suivante :

```
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]
```


Le tableau suivant décrit les options et les arguments de la commande `infacmd wfs createTables` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui exécute les flux de travail écrivant les métadonnées dans les tables.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

delegateTask

Attribue la propriété d'une instance de tâche humaine à un autre utilisateur ou un autre groupe.

Vous pouvez attribuer une instance de tâche à un autre utilisateur ou un autre groupe lorsque l'instance de tâche n'a pas de propriétaire. Ou bien, vous pouvez attribuer une instance de tâche à un autre utilisateur ou un autre groupe lorsque l'utilisateur actuel ne peut pas terminer l'instance de tâche.

Vous pouvez attribuer une instance de tâche à un utilisateur ou un groupe si vous êtes le propriétaire de l'instance de tâche ou l'administrateur d'entreprise de la tâche. Vous pouvez également attribuer l'instance de tâche à un autre utilisateur ou un autre groupe si vous êtes un propriétaire potentiel de l'instance de tâche. Vous êtes un propriétaire potentiel si vous faites partie d'un ensemble d'utilisateurs à qui la tâche humaine a attribué l'instance de tâche et qu'aucun utilisateur n'est propriétaire de la tâche.

Lorsque vous exécutez la commande `infacmd wfs delegateTask`, entrez l'ID de l'instance de tâche que vous voulez attribuer.

Pour trouver l'ID de l'instance de tâche, procédez de l'une des manières suivantes :

- Connectez-vous à Informatica Analyst et lisez l'ID de l'instance de tâche dans l'outil Monitoring tool.
- Exécutez la commande `infacmd wfs listTasks`.
- Demandez à l'administrateur d'entreprise ou à l'utilisateur propriétaire de l'instance de tâche. L'administrateur d'entreprise ou l'utilisateur peut lire l'ID de l'instance de tâche dans Informatica Analyst.

La commande `infacmd wfs delegateTask` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande `infacmd wfs delegateTask` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui exécute l'instance de flux de travail.

Option	Argument	Description
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-TaskID -tid	task_id	Requis. Identificateur de l'instance de tâche humaine à déléguer.
-Entity -to	to_entity	Requis. Nom de l'utilisateur ou du groupe dans le domaine auquel la commande doit déléguer l'instance de tâche. Par exemple, Native\Mary.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

dropTables

Annule les tables de base de données qui stockent les métadonnées d'exécution pour le flux de travail.

La commande dropTables utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments de la commande infacmd wfs dropTables :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	Mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ServiceName -sn	service_name	Requis. Nom du service qui exécute les flux de travail pour lesquels vous voulez supprimer des données.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

listActiveWorkflowInstances

Répertorie les instances de flux de travail actives. Une instance de flux de travail active est une instance sur laquelle une action peut être effectuée. Répertorie l'état, l'ID de l'instance de flux de travail, le nom de flux de travail et le nom de l'application de chaque instance de flux de travail active.

Les instances de flux de travail actives comprennent les instances de flux de travail en cours d'exécution et celles dont la récupération est activée et qui sont annulées.

La commande `infacmd wfs listActiveWorkflowInstances` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande `infacmd wfs listActiveWorkflowInstances` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données exécutant les instances de flux de travail.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

listMappingPersistedOutputs

Répertorie l'état de chaque sortie de mappage persistante. Vous pouvez mettre à jour les valeurs des sorties de mappage persistantes à l'aide de la commande `infacmd wfs setMappingPersistedOutputs`.

La commande `infacmd wfs listMappingPersistedOutputs` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd wfs listMappingPersistedOutputs` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui doit exécuter le flux de travail. L'application qui contient le flux de travail doit être déployée vers un service d'intégration de données.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire. Obligatoire. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation. Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application_name	Requis. Nom de l'application qui contient le flux de travail.
-Workflow -wf	workflow_name	Requis. Nom du flux de travail.
- mti	MappingTaskInstance	Requis. Nom d'une tâche de mappage qui a créé les sorties de mappage.

listTasks

Répertorie les instances de tâche humaines dans la base de données de flux de travail dans laquelle vous avez un rôle et qui répondent aux critères de filtrage que vous spécifiez. Utilisez les options de commande pour définir un ou plusieurs filtres.

Si vous ne définissez pas d'option de filtre, la commande renvoie une liste des dix premières instances de tâche humaine dans la base de données dans laquelle vous avez un rôle. Utilisez l'option `-MaxTasks` pour modifier le nombre d'instances de tâche renvoyées par la commande.

Vous avez un rôle dans une instance de tâche dans l'un des cas suivants :

- Vous êtes le propriétaire actuel de l'instance de tâche.
- Vous êtes un propriétaire potentiel d'une instance de tâche qu'un autre utilisateur ne possède pas. Par exemple, vous êtes membre d'un groupe dont les membres peuvent revendiquer la propriété de la tâche.
- Vous êtes l'administrateur d'entreprise de l'instance de tâche.

Les options de filtre que vous définissez pour la commande sont cumulatives. Si vous définissez plusieurs options de filtre, la commande renvoie une liste des instances de tâche humaine qui satisfont toutes les options que vous définissez.

La commande applique le nom d'utilisateur que vous soumettez en tant que filtre sur les instances de tâche dans la base de données de flux de travail. Par exemple, vous exécutez la commande `listTasks` avec le nom d'utilisateur « `Native\Mary` » et vous définissez l'option `-FilterByOwner` sur « `Native\John` ». La commande renvoie une liste des instances de tâche que John possède et pour lesquelles Mary est un propriétaire potentiel ou l'administrateur d'entreprise.

La commande `infacmd wfs listTasks` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande `infacmd wfs listTasks` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui exécute l'instance de flux de travail.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-MaxTasks -max	max_tasks	Facultatif. Définit une limite supérieure pour le nombre d'instances de tâche humaine dans la liste que la commande renvoie. Par défaut, la commande <code>infacmd wfs listTasks</code> renvoie une liste des dix premières instances de tâche. Vous pouvez utiliser l'option max en conjonction avec l'option -offset.
-FilterByOwner -ow	par exemple Native user_name	Facultatif. Filtre la liste des instances de tâche humaine dans la base de données de flux de travail par le nom de l'utilisateur ou du groupe qui possède la tâche.
-FilterByStatus -st	READY RESERVED IN_PROGRESS SUSPENDED	Facultatif. Filtre la liste des instances de tâche humaines dans la base de données de flux de travail par le statut de la tâche.
-FilterByCreationDate -cd	par exemple 2024-12-31	Facultatif. Filtre la liste des instances de tâche humaines dans la base de données de flux de travail par la date de création des tâches.
-FilterByType -tt	CleanseTask ClusterTask CleanseTaskReviewTask ClusterTaskReviewTask	Facultatif. Filtre la liste des instances de tâche humaines dans la base de données de flux de travail par le type de tâche.

Option	Argument	Description
-FilterByDueDate -dd	par exemple 2024-12-31	Facultatif. Filtre la liste des instances de tâche humaines dans la base de données de flux de travail en fonction de la date d'échéance de la tâche. La date d'échéance indique l'échéance actuelle pour l'achèvement des tâches.
-FilterByID -tid	par exemple 42	Facultatif. Filtre la liste des instances de tâche humaines dans la base de données de flux de travail par l'ID d'instance de tâche humaine.
-FilterByName -tn	par exemple « ExceptionStep {1-9} »	Facultatif. Filtre la liste des instances de tâche humaine dans la base de données de flux de travail par le nom d'instance de tâche humaine que vous spécifiez. Ne pas utiliser-FilterByName et-FilterByNameLike dans la même commande.
-FilterByNameLike -tnl	par exemple, « Step {%-}% »	Facultatif. Filtre la liste des instances de tâche humaine dans la base de données de flux de travail par le nom de la tâche humaine et autorise un caractère générique dans la chaîne de filtrage. Vous pouvez utiliser le caractère générique pour cent (%). Ne pas utiliser-FilterByName et-FilterByNameLike dans la même commande.
-TasksOffset -offset	tasks_offset	Facultatif. Spécifie un décalage de la première instance de tâche dans la liste des instances de tâche qui satisfont aux critères de filtrage. Lorsque vous spécifiez un décalage, la commande ignore les instances de tâche que le décalage spécifie et retourne une liste qui commence par l'instance de tâche suivante répondant aux critères de filtrage. Vous pouvez utiliser l'option -offset avec l'option -max pour organiser les résultats des commandes listTasks successives. Par exemple, si vous exécutez infacmd wfs listTasks avec une valeur -max de 50, vous renvoyez une liste d'instances de tâche dans la plage 1 à 50. Si vous exécutez la commande avec une valeur -max de 50 et une valeur de décalage de 51, vous renvoyez la liste des tâches dans la plage 51 à 100.
-Role	-role	Facultatif. Filtre la liste des instances de tâche humaine dans la base de données de flux de travail par le rôle de tâche humaine. Vous pouvez entrer les valeurs suivantes : - ADMINISTRATORS - ALL - OWNERS - POTENTIAL_OWNERS Si vous ne définissez pas l'option, la commande renvoie des instances de tâche pour tous les rôles.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

listWorkflowParams

Répertorie les paramètres pour un flux de travail et crée un fichier de paramètres que vous pouvez utiliser lorsque vous exécutez un flux de travail. La commande renvoie un fichier XML avec des valeurs par défaut que vous pouvez mettre à jour. Entrez le nom du fichier de paramètres lorsque vous exécutez le flux de travail avec la commande `infacmd wfs startWorkflow`.

La commande `infacmd wfs listWorkflowParams` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments infacmd wfs listWorkflowParams :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données pour exécuter le flux de travail. L'application qui contient le flux de travail doit être déployée dans un service d'intégration de données.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire. Obligatoire. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation. Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application_name	Obligatoire. Nom de l'application qui contient le flux de travail.
-Workflow -wf	workflow_name	Obligatoire. Nom du flux de travail.
- OutputFile -o	sortie file_to_write_to	Facultatif. Chemin et nom du fichier de paramètres à créer. Si vous ne spécifiez pas un fichier, la commande affiche les paramètres dans l'invite de commande.

Sortie listWorkflowParams

La commande listWorkflowParams renvoie un fichier de paramètres sous la forme d'un fichier XML avec des valeurs par défaut que vous pouvez mettre à jour.

Par exemple, vous exécutez la commande listWorkflowParams sur l'application « MyApp » et le flux de travail « MyWorkflow ». Le flux de travail « MyWorkflow » dispose d'un paramètre « MyParameter ».

La commande listWorkflowParams renvoie un fichier XML au format suivant :

```
<?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>
```

Le fichier XML de sortie contient les éléments de niveau supérieur suivants :

Élément d'application

Lorsque vous définissez un paramètre dans l'élément de niveau supérieur de l'application, le service d'intégration de données applique la valeur du paramètre lorsque vous exécutez le flux de travail spécifique dans l'application spécifique. Vous devez inclure au moins un élément de projet dans un élément d'application/flux de travail.

Par défaut, cet élément de niveau supérieur se trouve entre commentaires. Retirez les commentaires (! -- et -->) pour utiliser cet élément.

Élément de projet

Lorsque vous définissez un paramètre dans un élément de niveau supérieur du projet, le service d'intégration de données applique la valeur du paramètre au flux de travail spécifique dans le projet dans

toute application déployée. Le service applique également la valeur du paramètre à tout flux de travail qui utilise les objets dans le projet.

Si vous définissez le même paramètre dans un élément de projet ou d'application de niveau supérieur dans le même fichier de paramètres, la valeur des paramètres définie dans l'élément d'application est prioritaire.

listWorkflows

Répertorie les flux de travail dans une application.

La commande `infacmd wfs listWorkflows` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'`infacmd wfs listWorkflows` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données qui doit exécuter les flux de travail. L'application qui contient les flux de travail doit être déployée sur un service d'intégration de données.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire. Obligatoire. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation. Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application_name	Obligatoire. Nom de l'application qui contient les flux de travail.

pruneOldInstances

Supprime les données de processus de flux de travail de la base de données de flux de travail.

Lorsque le service d'intégration de données exécute un flux de travail, le processus de flux de travail enregistre les données de processus dans la base de données de processus. Avec le temps, la quantité de données de processus dans la base de données peut nuire aux performances de démarrage des processus de flux de travail. Pour supprimer les données de processus de la base de données, exécutez la commande wfs pruneOldInstances. Vous pouvez configurer la commande pour supprimer toutes les données de

processus dans la base de données de flux de travail. Ou, vous pouvez supprimer les données de processus générées par les flux de travail durant une période que vous spécifiez.

La commande `pruneOldInstances` supprime uniquement les données de processus. La commande ne supprime pas les données qu'une instance de flux de travail ou tout objet dans le flux de travail lit ou écrit. De même, la commande ne supprime pas les métadonnées d'objets de flux de travail.

Pour supprimer les données de processus, vous devez disposer du privilège Gérer le service sur le domaine.

La syntaxe de la commande `infacmd wfs pruneOldInstances` est la suivante :

```
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]
```

Le tableau suivant décrit les options et les arguments d'`infacmd wfs pruneOldInstances` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données exécutant l'instance de flux de travail.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-Days -d	days	<p>Période durant laquelle la commande supprime les données de processus.</p> <p>Pour calculer la période, la commande soustrait le nombre de jours que vous spécifiez de la date et heure d'exécution de la commande. La commande supprime toutes les données de processus générées par les processus de flux de travail durant la période.</p> <p>Entrez une valeur entre 0 et 24 855. Si vous entrez 0, la commande supprime toutes les données de processus dans la base de données de flux de travail.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>

recoverWorkflow

Récupère une instance de flux de travail. Vous pouvez récupérer une instance de flux de travail que vous avez annulée ou qui a été interrompue par une erreur récupérable. Lorsque vous récupérez une instance de flux de travail, le service d'intégration de données redémarre l'instance de flux de travail à la tâche interrompue et réexécute la tâche interrompue.

La commande `infacmd wfs recoverWorkflow` utilise la syntaxe suivante :

```
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]

```

Le tableau suivant décrit les options et arguments de la commande `infacmd wfs recoverWorkflow` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données ayant exécuté l'instance de flux de travail initiale.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-InstanceID -iid	ID de l'instance du flux de travail à récupérer	Requis. ID de l'instance du flux de travail à récupérer. Vous pouvez lire l'ID d'instance de flux de travail à partir des propriétés du flux de travail de l'onglet Surveillance de l'outil Administrator tool. Vous pouvez également exécuter la commande <code>infacmd wfs ListActiveWorkflowInstances</code> pour trouver l'ID d'instance de flux de travail.

Option	Argument	Description
-Wait -w	True False	Facultatif. Indique si la commande infacmd doit attendre la récupération de l'instance de flux de travail avant de retourner au shell ou à l'invite de commande. Si la valeur est True, la commande infacmd retourne au shell ou à l'invite de commande lorsque l'instance de flux de travail est récupérée. Vous ne pouvez pas exécuter les commandes suivantes tant que l'instance de flux de travail n'a pas été récupérée. Si la valeur est False, la commande infacmd retourne immédiatement au shell ou à l'invite de commande. Vous ne devez pas attendre la récupération de l'instance de flux de travail pour exécuter la commande suivante. La valeur par défaut est False.
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

releaseTask

Libère une instance de tâche humaine du propriétaire actuel. Vous pouvez libérer une instance de tâche si vous en êtes le propriétaire ou l'administrateur d'entreprise.

Lorsque vous libérez une instance de tâche, elle n'a pas de propriétaire. Si vous libérez une instance de tâche dont vous êtes le propriétaire, elle reste disponible dans l'outil Analyst tool. Si la tâche humaine identifie plusieurs utilisateurs comme propriétaires potentiels de l'instance de tâche que vous libérez, cette dernière est disponible pour tous les propriétaires potentiels.

La commande infacmd wfs releaseTask utilise la syntaxe suivante :

```
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]

```

Le tableau suivant décrit les options et arguments de la commande `infacmd wfs releaseTask` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui exécute l'instance de flux de travail.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-TaskID -tid	task_id	Requis. Identificateur de l'instance de tâche humaine dans la base de données de flux de travail.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

setMappingPersistedOutputs

Met à jour les sorties de mappage persistantes d'une instance de tâche de mappage dans un flux de travail. Ou, définit les sorties de mappage persistantes sur des valeurs Null. Les options de commande spécifient le nom de l'instance de tâche de mappage, le nom d'application et le nom de flux de travail.

Pour mettre à jour une valeur, entrez une paire nom-valeur qui contient le nom de sortie du mappage et la valeur vers laquelle effectuer la modification. Pour réinitialiser une valeur persistante sur des valeurs Null, utilisez l'option de réinitialisation. Vous pouvez réinitialiser quelques sorties de mappage ou toutes les sorties de mappage d'une instance de tâche de mappage. Pour afficher les sorties de mappage persistantes, utilisez la commande infacmd listMappingPersistedOutputs.

La commande infacmd wfs setMappingPersistedOutputs utilise la syntaxe suivante :

```
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]

```

Le tableau suivant décrit les options et les arguments de la commande `infacmd wfs setMappingPersistedOutputs` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui doit exécuter le flux de travail. L'application qui contient le flux de travail doit être déployée vers un service d'intégration de données.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Mot de passe -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire. Obligatoire. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p> <p>Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>
-Application -a	application_name	Requis. Nom de l'application qui contient le flux de travail.
-Workflow -wf	workflow_name	Requis. Nom du flux de travail.
-MappingTaskInstance -mti	mappingTaskInstancename	Requis. Nom d'une tâche de mappage qui a créé les sorties de mappage.
-outputvalues -onvp	space_separated_output_value_pairs	<p>Facultatif. Modifie la valeur persistante des sorties de mappage spécifiques. Entrez les paires nom-valeur séparées par un espace en suivant la syntaxe suivante : output_name=value output2_name=value output3_name=value</p>
-ResetOutputs -reset	reset_outputs	<p>Facultatif. Supprime la valeur de la sortie de mappage du référentiel. Pour réinitialiser des sorties de mappage spécifiques, entrez l'option de réinitialisation avec des noms de sortie de mappage séparés par un espace en suivant la syntaxe suivante :</p> <p>-reset mapping_output_name mapping_output2_name mapping_output3_name</p>

startTask

Démarre une instance de tâche humaine dans un flux de travail. L'opération de démarrage modifie le statut de l'instance de tâche en IN_PROGRESS.

La commande infacmd wfs startTask utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande infacmd wfs startTask :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui exécute l'instance de flux de travail.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-TaskID -tid	task_id	Requis. Identificateur de la tâche humaine à démarrer.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

startWorkflow

Démarre une instance d'un flux de travail. Vous pouvez exécuter plusieurs instances d'un flux de travail en même temps. Vous pouvez utiliser un ensemble ou un fichier de paramètres pour le flux de travail.

La commande `infacmd wfs startWorkflow` utilise la syntaxe suivante :

```
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]
```

La commande renvoie l'ID de l'instance de flux de travail.

Le tableau suivant décrit les options et arguments d'infacmd wfs startWorkflow :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui doit exécuter le flux de travail. L'application qui contient le flux de travail doit être déployée vers un service d'intégration de données.
-UserName -un	user_name	<p>Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>
-Password -pd	mot de passe	<p>Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p> <p>Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.</p>
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p> <p>Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.</p>

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-Application -a	application_name	Requis. Nom de l'application qui contient le flux de travail.
-Workflow -wf	workflow_name	Requis. Nom du flux de travail à démarrer.
-Wait -w	True False	Facultatif. Indique si la commande infacmd doit attendre que l'instance de flux de travail s'achève avant de retourner au shell ou à l'invite de commande. Si la valeur est True, la commande infacmd retourne au shell ou à l'invite de commande lorsque l'instance de flux de travail est terminée. Vous ne pouvez pas exécuter les commandes suivantes avant que l'instance de flux de travail ne soit terminée. Si la valeur est False, la commande infacmd retourne immédiatement au shell ou à l'invite de commande. Vous ne devez pas attendre que l'instance de flux de travail se termine pour exécuter la commande suivante. La valeur par défaut est False.
-ParameterFile -pf	parameter_file_path	Facultatif. Nom et chemin du fichier de paramètres. N'entrez pas un nom de fichier de paramètres et un nom d'ensemble de paramètres dans la même commande.
-ParameterSet -ps	parameter_set_name	Facultatif. Nom d'ensemble de paramètres à utiliser lors de l'exécution. L'option Ensemble de paramètres remplace n'importe quel ensemble de paramètres déployé avec l'application. N'entrez pas un nom de fichier de paramètres et un nom d'ensemble de paramètres dans la même commande.
-OperatingSystemProfile -osp	operating_system_profile_name	Facultatif. Nom du profil de système d'exploitation sous lequel le flux de travail s'exécute.

upgradeWorkflowParameterFile

Met à niveau un fichier de paramètres de flux de travail pour que le format de fichier soit compatible avec la version actuelle. Exécutez la commande dans les fichiers de paramètres de flux de travail que les utilisateurs ont créés dans une version Informatica 9.x. Lorsque vous exécutez la commande, vous identifiez un fichier de paramètres de flux de travail à mettre à niveau et vous spécifiez un fichier cible.

La commande infacmd wfs upgradeWorkflowParameterFile utilise la syntaxe suivante :

```
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

```

Le tableau suivant décrit les options et les arguments de la commande `infacmd wfs upgradeWorkflowParameterFile` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données qui doit exécuter le flux de travail. L'application qui contient le flux de travail doit être déployée vers un service d'intégration de données.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire. Requis. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p> <p>Facultatif. Nom du domaine de sécurité auquel appartient l'utilisateur. Le domaine de sécurité est sensible à la casse. La valeur par défaut est Natif.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>
-Application -a	application_name	Requis. Nom de l'application qui contient le flux de travail.
-Workflow -wf	workflow_name	Requis. Nom du flux de travail qui lit les valeurs du fichier de paramètre.
-Wait -w	True False	<p>Facultatif. Indique si la commande infacmd doit attendre que l'instance de flux de travail s'achève avant de retourner au shell ou à l'invite de commande. Si la valeur est True, la commande infacmd retourne au shell ou à l'invite de commande lorsque l'instance de flux de travail est terminée. Vous ne pouvez pas exécuter les commandes suivantes avant que l'instance de flux de travail ne soit terminée. Si la valeur est False, la commande infacmd retourne immédiatement au shell ou à l'invite de commande. Vous ne devez pas attendre que l'instance de flux de travail se termine pour exécuter la commande suivante. La valeur par défaut est False.</p>
-ParameterFile -pf	chemin du fichier de paramètres	Requis. Nom et emplacement du fichier de paramètre qui contient les valeurs à mettre à niveau.
-TargetOutputFile -of	chemin du fichier de paramètres	Requis. Nom et emplacement du fichier de sortie de la commande. Le fichier de sortie contient les paramètres valides pour la version actuelle.

CHAPITRE 39

Référence de commande infacmd WS

Ce chapitre comprend les rubriques suivantes :

- [ListOperationOptions, 1227](#)
- [ListOperationPermissions, 1229](#)
- [ListWebServiceOptions, 1231](#)
- [ListWebServicePermissions, 1233](#)
- [ListWebServices, 1235](#)
- [RenameWebService, 1236](#)
- [SetOperationPermissions, 1238](#)
- [SetWebServicePermissions, 1241](#)
- [StartWebService, 1244](#)
- [StopWebService, 1246](#)
- [UpdateOperationOptions, 1247](#)
- [UpdateWebServiceOptions, 1249](#)

ListOperationOptions

Répertorie les propriétés d'une opération de service Web qui est déployée vers un service d'intégration de données.

La commande `infacmd ws ListOperationOptions` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd ws ListOperationOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données où le service Web est déployé.
-UserName -un	user_name	<p>Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-WebService -ws	web_service	Obligatoire. Nom du service Web.
Opération -op	opération	Obligatoire. Nom de l'opération de service Web pour laquelle la liste de propriétés doit être créée.

ListOperationPermissions

Liste autorisations utilisateur et groupe pour une opération de service web. Vous devez indiquer des autorisations directes ou effectives.

La commande infacmd ws ListOperationPermissions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd ws ListOperationPermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données où le service Web est déployé.

Option	Argument	Description
-UserName -un	user_name	<p>Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>
-Password -pd	mot de passe	<p>Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p>
-SecurityDomain -sdn	security_domain	<p>Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-WebService -ws	web_service	Obligatoire. Nom du service Web.
-Operation -op	opération	Obligatoire. Nom de l'opération de service Web pour laquelle la liste de propriétés doit être créée.
-Direct ou -Effective	direct_permission_only effective_permission_only	Obligatoire. Entrez Direct pour lister les autorisations attribuées. Entrez Effective pour lister les autorisations héritées.

ListWebServiceOptions

Liste les propriétés d'un service Web qui est déployé dans un service d'intégration de données. Vous pouvez configurer les propriétés à l'aide de l'outil Administrator ou infacmd ws UpdateWebServiceOptions.

La commande infacmd ws ListWebServiceOptions utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd ws ListWebServiceOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données où le service Web est déployé.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-WebService -ws	web_service	Obligatoire. Nom du service Web.

ListWebServicePermissions

Liste les autorisations de groupe et d'utilisateur pour un service web qui est déployé vers un service d'intégration de données. Vous devez indiquer des autorisations directes ou effectives.

Le tableau suivant décrit les options et arguments d'infacmd ws ListWebServicePermissions :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd ws ListWebServicePermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données où le service Web est déployé.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-WebService -ws	web_service	Obligatoire. Nom du service Web.
-Direct ou -Effective	direct_permission_only effective_permission_only	Obligatoire. Entrez Direct pour lister les autorisations attribuées. Entrez Effective pour lister les autorisations héritées.

ListWebServices

Répertorie les services Web d'une application. Si vous n'entrez pas un nom d'application, infacmd liste tous les services Web pour un service d'intégration de données.

La commande infacmd ws ListWebServices utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd ws ListWebServices :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données où les services Web sont déployés.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-application -ap	application	Facultatif. Nom de l'application dont les services Web doivent être répertoriés.

RenameWebService

Renomme un service Web.

La commande infacmd ws RenameWebService utilise la syntaxe suivante :

```

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

```


Le tableau suivant décrit les options et arguments d'infacmd ws RenameWebService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données où le service Web est déployé.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-WebService -ws	web_service	Obligatoire. Nom du service Web.
-NewName -n	new_name	Obligatoire. Nouveau nom pour le service Web.

SetOperationPermissions

Définit les autorisations d'utilisateur ou de groupe pour une opération de service Web. Vous pouvez définir ou refuser des autorisations pour un utilisateur ou un groupe.

La commande `infacmd ws SetOperationPermissions` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd ws SetOperationPermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel le service Web est déployé.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>
-WebService -ws	web_service	Requis. Nom du service Web.
-Operation -op	operation	Requis. Nom de l'opération de service Web.
-GranteeUserName GranteeGroupName -gun -ggn	grantee_user_name grantee_group_name	Requis. Nom d'utilisateur ou nom de groupe pour lequel définir ou refuser des autorisations.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Requis si vous utilisez une authentification LDAP et que vous attribuez des autorisations d'utilisateur. Nom du domaine de sécurité auquel appartient l'utilisateur.

Option	Argument	Description
-AllowedPermissions -ap	list_of_allowed_permissions_separated_by_space	Requis. Liste des autorisations à autoriser. Entrez les paramètres suivants séparés par une espace : <ul style="list-style-type: none"> - GRANT. Les utilisateurs peuvent accorder et retirer des autorisations sur l'opération à l'aide de l'outil Administrator ou en utilisant le programme de ligne de commande infacmd. - EXECUTE. Les utilisateurs peuvent exécuter l'opération.
-DeniedPermissions -dp	list_of_denied_permissions_separated_by_space	Facultatif. Liste des autorisations pour refuser des utilisateurs. Entrez les paramètres suivants séparés par une espace : <ul style="list-style-type: none"> - GRANT. Les utilisateurs ne peuvent pas accorder ou retirer des autorisations sur l'opération. - EXECUTE. Les utilisateurs ne peuvent pas exécuter l'opération.

SetWebServicePermissions

Définit les autorisations d'utilisateur ou de groupe pour un service Web. Vous pouvez définir ou refuser des autorisations pour un utilisateur ou un groupe.

La commande `infacmd ws SetWebServicePermissions` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infacmd ws SetWebServicePermissions :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service d'intégration de données dans lequel le service Web est déployé.
-UserName -un	user_name	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	password	Requis si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-ResilienceTimeout -re	timeout_period_in_seconds	<p>Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.</p>
-WebService -ws	web_service	Requis. Nom du service Web.
-GranteeUserName GranteeGroupName -gun -ggn	grantee_user_name grantee_group_name	Requis. Nom d'utilisateur ou nom de groupe pour lequel définir ou refuser des autorisations.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Requis si vous utilisez une authentification LDAP et que vous attribuez des autorisations d'utilisateur. Nom du domaine de sécurité auquel appartient l'utilisateur.

Option	Argument	Description
-AllowedPermissions -ap	list_of_allowed_permissions_separated_by_space	Requis. Liste des autorisations à autoriser. Entrez les paramètres suivants séparés par une espace : - GRANT. Les utilisateurs peuvent accorder et retirer des autorisations sur le service Web à l'aide de l'outil Administrator ou en utilisant le programme de ligne de commande infacmd. - EXECUTE. Les utilisateurs peuvent exécuter le service Web.
-DeniedPermissions -dp	list_of_denied_permissions_separated_by_space	Facultatif. Liste des autorisations pour refuser des utilisateurs. Entrez les paramètres suivants séparés par une espace : - GRANT. Les utilisateurs ne peuvent pas accorder ou retirer des autorisations sur le service Web. - EXECUTE. Les utilisateurs ne peuvent pas exécuter le service Web.

StartWebService

Démarre un service Web qui est déployé dans un service d'intégration de données.

La commande infacmd ws StartWebService utilise la syntaxe suivante :

```
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
```


Le tableau suivant décrit les options et arguments d'infacmd ws StartWebService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Nom du service d'intégration de données où le service Web est déployé.
-WebService -ws	web_service	Obligatoire. Nom du service Web à démarrer.

StopWebService

Arrête un service Web exécuté.

La commande infacmd ws StopWebService utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd ws StopWebService :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-ServiceName -sn	service_name	Nom du service d'intégration de données où le service Web est déployé.
-WebService -ws	web_service	Obligatoire. Nom du service Web à arrêter.

UpdateOperationOptions

Met à jour les propriétés d'une opération de service Web qui est déployée vers un service d'intégration de données.

La commande `infacmd ws UpdateOperationOptions` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments d'infacmd ws UpdateOperationOptions :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement INFA_DEFAULT_DOMAIN. Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données où le service Web est déployé.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.
-WebService -ws	web_service	Obligatoire. Nom du service Web.

Option	Argument	Description
Opération -op	opération	Obligatoire. Nom de l'opération de service Web à mettre à jour.
-Options -o> options	options	Entrez l'option de service Web au format suivant : ... -o option_type.option_name=value

Options d'opération

Utilisez les options d'opération pour mettre à jour une opération de service Web. Utilisez les options d'opération avec `infacmd ws UpdateOperationOptions`.

Entrez les options d'opération au format suivant :

```
... -o OperationOptions.option_name=value ...
```

Le tableau suivant décrit une option pour `infacmd ws UpdateOperationOptions` :

Option	Description
<code>WebServiceOperationOptions.ResultSetCacheExpirationPeriod</code>	Quantité de temps en millisecondes pendant laquelle le cache de l'ensemble de résultats est utilisable. Si défini sur -1, le cache n'expire jamais. Si défini sur 0, la mise en cache de l'ensemble des résultats est désactivée. Si vous voulez que tous les caches utilisent la même période d'expiration, purgez le cache de l'ensemble des résultats après avoir modifié la période d'expiration. Par défaut 0.

UpdateWebServiceOptions

Actualise les propriétés d'un service Web qui est déployé vers un service d'intégration de données. Pour afficher les propriétés du service Web, vous pouvez utiliser `infacmd ws ListWebServiceOptions`.

La commande `infacmd ws UpdateWebServiceOptions` utilise la syntaxe suivante :

```
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
```

Le tableau suivant décrit les options et arguments de la commande `infacmd ws UpdateWebServiceOptions` :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option -dn ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option -dn est prioritaire.
-ServiceName -sn	service_name	Obligatoire. Nom du service d'intégration de données où le service Web est déployé.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-Password -pd	mot de passe	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel <code>infacmd</code> tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Option	Argument	Description
-WebService -ws	web_service	Obligatoire. Nom du service Web.
-Options -o> options	options	Entrez chaque option en la séparant par un espace.

Options du service Web

Utilisez une syntaxe spécifique pour entrer les options du service Web.

Entrez les options du service Web dans le format suivant :

```
... -o option_type.option_name=value
```

Pour entrer plusieurs options, séparez-les par un espace. Pour saisir une valeur qui contient un espace ou un autre caractère non alphanumérique, placez la valeur entre guillemets.

Le tableau suivant décrit les options du service Web :

Option	Description
WebServiceOptions.startupType	Détermine si le service Web est activé pour s'exécuter lorsque l'application démarre ou lorsque vous démarrez le service Web. Entrez enabled ou disabled.
WebServiceOptions.traceLevel	Niveau des messages d'erreur écrits dans le journal d'exécution du service Web. Choisissez l'un des niveaux de message suivants : <ul style="list-style-type: none"> - OFF - SEVERE - WARNING - INFO - FINE - FINEST - ALL
WebServiceOptions.requestTimeout	Temps maximal en millisecondes d'exécution par le service d'intégration de données d'une opération de mappage avant l'expiration de la demande de service Web. La valeur par défaut est 3 600 000.
WebServiceOptions.maxConcurrentRequests	Nombre maximal de demandes qu'un service Web peut traiter simultanément. La valeur par défaut est 10.
WebServiceOptions.sortOrder	Ordre de tri utilisé par le service d'intégration de données pour trier et comparer les données lorsqu'il s'exécute en mode Unicode. La valeur par défaut est binaire.
WebServiceOptions.EnableTransportLayerSecurity	Indique que le service Web doit utiliser HTTPS. Si le service d'intégration de données n'est pas configuré pour utiliser HTTPS, le service Web ne démarre pas. Entrez true ou false.

Option	Description
WebServiceOptions.EnableWSSecurity	Active le service d'intégration de données afin de valider les justificatifs d'identité de l'utilisateur et de vérifier que ce dernier est autorisé à exécuter chaque opération de service Web. Entrez true ou false.
WebServiceOptions.optimizeLevel	<p>Niveau d'optimisation que le service d'intégration de données applique à l'objet. Entrez la valeur numérique associée au niveau d'optimisation que vous voulez configurer. Vous pouvez entrer l'une des valeurs numériques suivantes :</p> <ul style="list-style-type: none"> - 0. Le service d'intégration de données n'applique pas d'optimisation. - 1. Le service d'intégration de données applique la méthode d'optimisation de projection précoce. - 2. Le service d'intégration de données applique les méthodes d'optimisation de projection précoce, de sélection précoce, push-into et de prédicat. - 3. Le service d'intégration de données applique les méthodes d'optimisation de projection précoce, de sélection précoce, push-into, de prédicat et de semi-jointure basées sur les coûts.
WebServiceOptions.DTMKeepAliveTime	<p>Nombre de millisecondes pendant lesquelles l'instance DTM demeure ouverte après le traitement de la dernière demande. Les demandes de service Web émises pour la même opération peuvent réutiliser l'instance ouverte. Utilisez le délai keepalive pour améliorer les performances lorsque le délai requis pour traiter la demande est limité par rapport au délai d'initialisation de l'instance DTM. Si la demande échoue, l'instance DTM prend fin.</p> <p>Doit être un nombre entier. Une valeur entière négative indique que l'intervalle de temps Garder actif DTM pour le service d'intégration de données est utilisé. 0 signifie que le service d'intégration de données ne conserve pas l'instance DTM en mémoire. Valeur par défaut : -1.</p>

CHAPITRE 40

Référence de la commande infacmd xrf

Ce chapitre comprend les rubriques suivantes :

- [generateReadableViewXML, 1253](#)
- [updateExportXML, 1254](#)

generateReadableViewXML

Génère un fichier XML accessible en lecture depuis un fichier XML d'exportation. Le fichier XML d'exportation peut contenir le domaine exporté ou le contenu du référentiel modèle.

La commande `infacmd xrf generateReadableViewXML` simplifie le processus de modification d'un fichier XML d'exportation en exposant les valeurs à modifier. Utilisez le fichier XML accessible en lecture pour modifier des valeurs générées à partir du fichier XML d'exportation. Par exemple, si vous exportez un mappage enregistré dans le référentiel modèle, vous pouvez modifier le nom des colonnes ou modifier la précision et l'échelle des types de données. Si vous souhaitez apporter des modifications structurelles aux valeurs dans le fichier XML d'exportation, utilisez l'outil Administrator tool ou l'outil Developer tool selon que vous ayez exporté le contenu du domaine ou du référentiel modèle.

La commande `infacmd xrf generateReadableViewXML` utilise la syntaxe suivante :

```
generateReadableViewXML  
  
<-SourceExportFile|-sxf> source_export_file  
  
<-TargetFile|-tf> target_file_Name
```

Le tableau suivant décrit les options et arguments d'`infacmd xrf generateReadableViewXML` :

Option	Argument	Description
-SourceExportFile -sxf	source_export_file	Obligatoire. Chemin et nom du fichier XML d'exportation.
-TargetFile -tf	target_file_Name	Obligatoire. Chemin et nom du fichier XML accessible en lecture.

updateExportXML

Met à jour un fichier d'exportation XML avec les modifications apportées au fichier XML correspondant, accessible en lecture. Vous pouvez mettre à jour un fichier XML accessible en lecture qui contient le contenu de référentiel modèle et régénérer le fichier d'exportation XML avec les modifications.

La commande `infacmd xrf updateExportXML` utilise la syntaxe suivante :

```
updateExportXML  
  
<SourceExportFile|-sxf> source_file  
<generatedViewFile|-vf> view_file  
<TargetFile|-tf> target_file_Name
```

Le tableau suivant décrit les options et arguments de la commande `infacmd xrf updateExportXML` :

Option	Argument	Description
-SourceExportFile -sxf	source_file	Requis. Chemin et nom du fichier XML d'exportation.
-generatedViewFile -vf	view_file	Requis. Chemin et nom du fichier XML accessible en lecture contenant les modifications requises.
-TargetFile -tf	target_file_Name	Requis. Chemin et nom du fichier d'exportation XML mis à jour.

CHAPITRE 41

Fichiers de contrôle infacmd

Ce chapitre comprend les rubriques suivantes :

- [Présentation des fichiers de contrôle infacmd, 1255](#)
- [Configuration du fichier de contrôle, 1256](#)
- [Fichiers de contrôle d'exportation, 1257](#)
- [Fichiers de contrôle d'importation, 1261](#)
- [Règles et directives concernant les fichiers de contrôle, 1269](#)
- [Exemples de fichier de contrôle pour les objets de domaine, 1270](#)
- [Exemples de fichier de contrôle pour les objets du référentiel modèle, 1271](#)

Présentation des fichiers de contrôle infacmd

Lorsque vous utilisez le programme de ligne de commande infacmd pour exporter et importer des objets, vous pouvez utiliser un fichier de contrôle pour filtrer les objets exportés ou importés par la commande.

Vous pouvez utiliser les fichiers de contrôle suivants avec la commande infacmd :

- Fichier de contrôle d'exportation. Utilisez un fichier de contrôle d'exportation pour spécifier les objets du domaine ou du référentiel modèle à exporter vers un fichier d'exportation.
- Fichier de contrôle d'importation. Utilisez un fichier de contrôle d'importation pour spécifier les objets du référentiel modèle à importer vers un fichier d'importation.
- Fichiers de contrôle d'importation. Utilisez un fichier de contrôle d'importation pour spécifier les objets à importer depuis le fichier d'exportation dans le domaine ou le référentiel modèle.
- Fichiers de contrôle d'importation. Utilisez un fichier de contrôle d'importation pour spécifier les objets à importer depuis le fichier d'exportation dans le référentiel modèle.

Si vous n'utilisez pas de fichier de contrôle d'exportation pendant l'export, infacmd ne filtre pas les objets exportés à partir du domaine ou du projet de référentiel modèle spécifié. Si vous n'utilisez pas de fichier de contrôle d'importation lors de l'import dans le domaine, infacmd importe tous les objets inclus dans le fichier d'exportation. Si vous n'utilisez pas de fichier de contrôle d'importation lors de l'import dans le référentiel modèle, infacmd importe tous les objets inclus dans le projet spécifié du fichier d'exportation.

Si vous n'utilisez pas de fichier de contrôle d'exportation pendant l'exportation, infacmd ne filtre pas les objets exportés à partir du projet de référentiel modèle spécifié. Si vous n'utilisez pas de fichier de contrôle d'importation lors de l'import dans le référentiel modèle, infacmd importe tous les objets inclus dans le projet spécifié du fichier d'exportation.

Configuration du fichier de contrôle

Un fichier de contrôle est un fichier XML basé sur un fichier de schéma d'import ou d'export. Vous pouvez créer un fichier de contrôle basé sur les fichiers de schéma suivants :

- exportControl.xsd. Définit la mise en page et la syntaxe des fichiers de contrôle d'exportation.
- importControl.xsd. Définit la mise en page et la syntaxe des fichiers de contrôle d'importation.

Vous pouvez accéder aux fichiers de schéma en tant que partie du fichier oie-util.jar dans le répertoire d'installation suivant :

```
<InformaticaInstallationDir>/services/shared/jars/shapp
```

Pour accéder aux fichiers exportControl.xsd. et importControl.xsd. depuis la ligne de commande, accédez au fichier oie-util.jar et faites une extraction du fichier JAR à l'aide de la commande suivante :

```
jar -xvf <jar_name>
```

En outre, vous pouvez extraire le fichier JAR oie-util avec un logiciel de décompression, tel que WinRAR, ou afficher les fichiers XSD depuis le fichier JAR oie-util à l'aide du décompilateur Java pour accéder aux fichiers de schéma.

Pour créer un fichier de contrôle d'exportation, créez un fichier XML basé sur le fichier de schéma exportControl.xsd. Le fichier doit commencer par une déclaration XML et par l'emplacement dans l'élément racine exportParams du fichier de schéma hébergé. Inclure les lignes suivantes dans le fichier :

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
...
</exportParams>
```

Pour créer un fichier de contrôle d'importation, créez un fichier XML basé sur le fichier de schéma importControl.xsd. Le fichier doit commencer par une déclaration XML et par l'emplacement dans l'élément racine importParams du fichier de schéma hébergé. Inclure les lignes suivantes dans le fichier :

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
...
</importParams>
```

Inclure les éléments et les attributs restants dans le fichier XML en fonction des objets que vous souhaitez exporter ou importer.

Conventions de nommage du fichier de contrôle

Donnez aux fichiers de contrôle un nom de fichier facilement identifiable.

Ajoutez un préfixe à chaque nom de fichier pour indiquer s'il s'agit d'un fichier de contrôle d'exportation ou d'importation. Par exemple, utilisez les suggestions de conventions de nommage suivantes :

- ecf_<file_name>.xml pour les fichiers de contrôle d'exportation
- icf_<file_name>.xml pour les fichiers de contrôle d'importation

Pour les fichiers de contrôle des objets du domaine, vous pouvez aussi inclure dans le nom de fichier le type d'objet considéré pour l'exportation ou l'importation.

Fichiers de contrôle d'exportation

Un fichier de contrôle d'exportation est un fichier XML que vous utilisez avec les commandes infacmd. Le fichier de contrôle filtre les objets exportés par infacmd depuis un domaine ou un référentiel modèle. Un fichier de contrôle d'exportation est un fichier XML que vous utilisez avec les commandes infacmd. Le fichier de contrôle filtre les objets exportés par infacmd depuis un référentiel modèle.

Vous pouvez utiliser un fichier de contrôle d'exportation avec les commandes suivantes :

Vous pouvez utiliser un fichier de contrôle d'exportation avec les commandes suivantes :

infacmd isp ExportDomainObjects

Exporte les utilisateurs natifs, les groupes natifs, les rôles, les connexions et les configurations de cluster depuis le domaine vers un fichier d'exportation au format XML. Lorsque vous spécifiez un fichier de contrôle d'exportation à la commande, vous filtrez les objets que vous voulez exporter. Par exemple, utilisez un fichier de contrôle pour exporter tous les objets créés après une certaine date ou pour exporter uniquement les connexions en excluant tout autre type d'objets.

infacmd oie ExportObjects

Exporte tous les types d'objets du référentiel modèle depuis un projet spécifié vers un fichier d'exportation au format XML. Lorsque vous spécifiez un fichier de contrôle d'exportation à la commande, vous filtrez les objets que vous voulez exporter. Par exemple, utilisez un fichier de contrôle pour exporter tous les objets créés par un utilisateur spécifique ou pour exporter des types d'objets spécifiques du projet.

Infacmd ne permet pas l'export de dossiers vides. Lors de l'exportation d'objets du référentiel modèle, infacmd exporte aussi les objets dépendants. Un objet dépendant est un objet utilisé par un autre objet. Les objets dépendants peuvent être dans le même projet ou dans d'autres projets.

Un fichier de contrôle d'exportation utilise des paramètres différents selon que vous configurez le fichier pour exporter des objets de domaine ou des objets du référentiel modèle.

Un fichier de contrôle d'exportation utilise des paramètres différents selon que vous configurez le fichier pour exporter des objets du référentiel modèle.

Paramètres du fichier de contrôle d'exportation pour les objets de domaine

Utilisez les paramètres du fichier de contrôle d'exportation pour configurer les objets du domaine que vous voulez exporter.

Un fichier de contrôle d'exportation pour les objets de domaine peut contenir les éléments suivants :

- exportParams. Peut contenir plusieurs éléments objectList.
- objectList. Contient les attributs pour filtrer les objets par type. Peut contenir plusieurs éléments objet.
- objet. Contient un attribut pour filtrer les objets par nom.

Le tableau suivant répertorie les éléments du fichier de contrôle d'exportation dont les attributs sont configurables :

Élément	Nom de l'attribut	Description de l'attribut
objectList	type	Requis. Type d'objet de domaine à exporter. Spécifiez l'une des valeurs suivantes : <ul style="list-style-type: none"> - Utilisateur - Groupe - Rôle - Configuration de cluster. - Connexion La valeur n'est pas sensible à la casse.
objectList	createdBefore	Facultatif. Date et heure. Exporte les objets du type spécifié créés avant cette date et heure. Entrez la date et l'heure dans le format suivant : yyyy-MM-dd HH:mm:ssZ
objectList	createdAfter	Facultatif. Date et heure. Exporte les objets du type spécifié créés après cette date et heure. Entrez la date et l'heure dans le format suivant : yyyy-MM-dd HH:mm:ssZ
objectList	lastUpdatedBefore	Facultatif. Date et heure. Exporte les objets du type spécifié mis à jour avant cette date et heure. Entrez la date et l'heure dans le format suivant : yyyy-MM-dd HH:mm:ssZ
objectList	lastUpdatedAfter	Facultatif. Date et heure. Exporte les objets du type spécifié mis à jour après cette date et heure. Entrez la date et l'heure dans le format suivant : yyyy-MM-dd HH:mm:ssZ
objet	name	Requis. Nom de l'objet à exporter. Si un attribut « time » est associé à l'élément conteneur objectList, infacmd exporte les objets qui correspondent à la fois au nom d'objet spécifié et au filtre « time ». La valeur n'est pas sensible à la casse.

Exemple de fichier de contrôle d'exportation pour les objets de domaine

Le code suivant montre un exemple de fichier de contrôle d'exportation pour les objets de domaine :

```
<?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>
```

Paramètres du fichier de contrôle d'exportation pour les objets du référentiel modèle

Utilisez les paramètres du fichier de contrôle d'exportation pour configurer les objets que vous voulez exporter depuis le référentiel modèle.

Un fichier de contrôle d'exportation pour les objets du référentiel modèle peut contenir les éléments suivants :

- exportParams. Peut contenir un seul élément dossiers.
- dossiers. Peut contenir plusieurs éléments dossier.
- dossier. Contient les attributs permettant de filtrer les objets d'un dossier spécifique. Peut contenir plusieurs éléments objectList.
- objectList. Contient les attributs pour filtrer les objets par type. Peut contenir plusieurs éléments objet.
- objet. Contient un attribut pour filtrer les objets par nom.

Le tableau suivant décrit les attributs configurables pour l'élément de dossier dans le fichier de contrôle d'exportation :

Nom d'attribut	Description de l'attribut
chemin	Facultatif. Chemin d'accès du dossier contenant les objets que vous voulez exporter. Utiliser le format suivant : "/<folder_name>/<folder_name>" Par exemple, si un projet contient un dossier nommé F1, le chemin d'accès du dossier F1 est « /F1 ». Pour exporter tous les objets du projet, spécifiez « / ». La valeur n'est pas sensible à la casse. La valeur par défaut est « / ».
récuratif	Facultatif. Indique si les objets des sous-dossiers du dossier spécifié doivent être exportés. Défini sur « Vrai » pour exporter à partir des sous-dossiers. Les valeurs valides sont « Vrai » et « Faux ». Cette valeur est sensible à la casse. La valeur par défaut est True.
sélectionner	Facultatif. Indique si infacmd exporte tous les objets restants dans le dossier spécifié lorsque vous définissez un élément objectList pour le dossier. Définir « Tous » pour exporter tous les objets restants. Par exemple, les lignes suivantes exportent les mappages créés par user1. Les lignes exportent tous les objets restants du dossier spécifié : <pre><folder path="/Testfolder" select="all"> <objectList type="Mapping" createdBy="user1" /> </folder></pre> Si vous définissez un élément objectList sans utiliser l'attribut « Sélectionner », infacmd exporte les objets qui satisfont les attributs définis dans objectList. Par exemple, les lignes suivantes exportent les mappages créés par user1 dans le dossier spécifié : <pre><folder path="/Testfolder"> <objectList type="Mapping" createdBy="user1" /> </folder></pre> Si vous ne définissez pas d'élément objectList pour le dossier, la valeur par défaut de l'attribut « Sélectionner » est « Tous ». Par exemple, la ligne suivante exporte tous les objets du dossier spécifié : <pre><folder path="/Testfolder" /></pre> La valeur valide est « Tous ».
createdBy	Facultatif. Nom d'utilisateur. Exporte les objets créés par cet utilisateur. La valeur n'est pas sensible à la casse.

Nom d'attribut	Description de l'attribut
createdBefore	Facultatif. Date et heure. Exporte les objets créés avant cette date et heure. Entrez la date et l'heure dans le format suivant : yyyy-MM-dd HH:mm:ssZ
createdAfter	Facultatif. Date et heure. Exporte les objets créés après cette date et heure. Entrez la date et l'heure dans le format suivant : yyyy-MM-dd HH:mm:ssZ
lastUpdatedBefore	Facultatif. Date et heure. Exporte les objets mis à jour avant cette date et heure. Entrez la date et l'heure dans le format suivant : yyyy-MM-dd HH:mm:ssZ
lastUpdatedAfter	Facultatif. Date et heure. Exporte les objets mis à jour après cette date et heure. Entrez la date et l'heure dans le format suivant : yyyy-MM-dd HH:mm:ssZ
lastUpdatedBy	Facultatif. Nom d'utilisateur. Exporte les objets dont la dernière mise à jour a été effectuée par cet utilisateur. La valeur n'est pas sensible à la casse.

Le tableau suivant décrit les attributs configurables pour l'élément objectList dans le fichier de contrôle d'exportation :

Nom d'attribut	Description de l'attribut
type	Obligatoire. Type d'objet du référentiel modèle à exporter depuis le chemin d'accès du dossier spécifié. Les valeurs valides comprennent tous les types d'objets présents dans le référentiel modèle. Vous pouvez afficher le type de l'objet dans la vue Propriétés de l'outil Developer. Par exemple, vous pouvez entrer « Objet de données relationnel » ou « Profil ». La valeur n'est pas sensible à la casse.
createdBy	Facultatif. Nom d'utilisateur. Exporte les objets du type spécifié créés par cet utilisateur. La valeur n'est pas sensible à la casse.
createdBefore	Facultatif. Date et heure. Exporte les objets du type spécifié créés avant cette date et heure. Entrez la date et l'heure dans le format suivant : yyyy-MM-dd HH:mm:ssZ
createdAfter	Facultatif. Date et heure. Exporte les objets du type spécifié créés après cette date et heure. Entrez la date et l'heure dans le format suivant : yyyy-MM-dd HH:mm:ssZ
lastUpdatedBefore	Facultatif. Date et heure. Exporte les objets du type spécifié mis à jour avant cette date et heure. Entrez la date et l'heure dans le format suivant : yyyy-MM-dd HH:mm:ssZ

Nom d'attribut	Description de l'attribut
lastUpdatedAfter	Facultatif. Date et heure. Exporte les objets du type spécifié mis à jour après ces date et heure. Entrez la date et l'heure dans le format suivant : yyyy-MM-dd HH:mm:ssZ
lastUpdatedBy	Facultatif. Nom d'utilisateur. Exporte les objets du type spécifié dont la dernière mise à jour a été effectuée par cet utilisateur. La valeur n'est pas sensible à la casse.

Le tableau suivant décrit l'attribut configurable pour l'élément d'objet dans le fichier de contrôle d'exportation :

Nom d'attribut	Description de l'attribut
nom	Obligatoire. Nom de l'objet à exporter. Si l'élément conteneur objectList inclut un attribut « Utilisateur » ou « Heure », infacmd exporte les objets qui correspondent à la fois au nom d'objet spécifié et au filtre « Utilisateur » ou « Heure ». Cette valeur est sensible à la casse.

Exemple de fichier de contrôle d'exportation pour les objets du référentiel modèle

Le code suivant montre un exemple de fichier de contrôle d'exportation pour les objets du référentiel modèle :

```
<?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>
```

Fichiers de contrôle d'importation

Un fichier de contrôle d'importation est un fichier XML que vous utilisez avec les commandes infacmd. Le fichier de contrôle filtre les objets importés par infacmd depuis un fichier d'exportation vers un domaine ou un référentiel modèle. Un fichier de contrôle d'importation est un fichier XML que vous utilisez avec les commandes infacmd. Le fichier de contrôle filtre les objets importés par infacmd depuis un fichier d'exportation vers un référentiel modèle.

Vous pouvez utiliser un fichier de contrôle d'importation avec les commandes suivantes :

Vous pouvez utiliser un fichier de contrôle d'importation avec la commande suivante :

infacmd isp ImportDomainObjects

Importe des utilisateurs natifs, des groupes natifs, des rôles, des connexions et des configurations de cluster depuis un fichier d'exportation dans un domaine. Lorsque vous spécifiez un fichier de contrôle d'importation à la commande, vous pouvez effectuer les tâches suivantes :

- Filtrez les objets que vous voulez importer. Par exemple, utilisez le fichier de contrôle pour importer un type d'objet spécifique.
- Configurez les stratégies de résolution de conflit pour des types d'objets spécifiques ou des objets spécifiques.

infacmd oie ImportObjects

Importe dans un référentiel modèle les objets du référentiel modèle depuis un fichier d'exportation. Lorsque vous spécifiez un fichier de contrôle d'importation à la commande, vous pouvez effectuer les tâches suivantes :

- Filtrez les objets que vous voulez importer. Par exemple, utilisez le fichier de contrôle pour importer un type d'objet spécifique.
- Configurez les stratégies de résolution de conflit pour des types d'objets spécifiques ou des objets spécifiques.
- Mappez les connexions dans le référentiel source sur les connexions dans le référentiel cible.

Il peut exister des objets du référentiel modèle dépendants dans d'autres dossiers ou projets. Vous devez inclure tous les objets dépendants à l'aide des éléments `folderMap` dans le fichier de contrôle d'importation. Dans le cas contraire, l'importation peut échouer avec un message d'erreur, car un objet dépendant n'existe pas dans le référentiel cible.

Vous pouvez définir une stratégie de résolution de conflit par l'intermédiaire de la ligne de commande ou du fichier de contrôle lorsque vous importez les objets. Dans le cas où une résolution de conflit est définie à la fois dans la ligne de commande et dans le fichier de contrôle, le fichier de contrôle est prioritaire. L'importation échoue lorsqu'il y a un conflit et que vous n'avez pas défini de stratégie de résolution de conflit.

Si vous définissez le renommer la stratégie de résolution de conflit « rename », vous pouvez indiquer un nom dans le fichier de contrôle pour un objet spécifique. Ou `infacmd` peut générer un nom en adjoignant un numéro séquentiel à la fin du nom.

Un fichier de contrôle d'importation utilise des paramètres différents selon que vous configurez le fichier pour importer des objets de domaine ou des objets du référentiel modèle.

Un fichier de contrôle d'importation utilise des paramètres différents selon que vous configurez le fichier pour importer des objets de domaine ou des objets du référentiel modèle.

Paramètres du fichier de contrôle d'importation pour les objets de domaine

Utilisez les paramètres du fichier de contrôle d'importation pour configurer les objets que vous voulez importer dans le domaine depuis un fichier XML.

Un fichier de contrôle d'importation pour les objets de domaine peut contenir les éléments suivants :

- `importParams`. Peut contenir plusieurs éléments `objectList`.
- `objectList`. Contient les attributs pour filtrer les objets par type. Peut contenir plusieurs éléments `objet`.
- `objet`. Contient les attributs pour filtrer les objets par nom.

Le tableau suivant répertorie les éléments du fichier de contrôle d'importation dont les attributs sont configurables :

Élément	Nom de l'attribut	Description de l'attribut
objectList	type	<p>Requis. Type d'objet de domaine que vous voulez importer. Spécifiez l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> - Utilisateur - Groupe - Rôle - Configuration de cluster - Connexion <p>La valeur n'est pas sensible à la casse.</p>
objectList	select	<p>Facultatif. Indique si infacmd importe tous les objets restants du type spécifié lorsque vous définissez un élément d'objet pour objectList. Définissez « all » pour importer tous les objets restants. Par exemple, les lignes suivantes importent Group1 avec une stratégie de résolution « Réutiliser ». Les lignes importent tous les groupes restants avec une stratégie de résolution « Fusionner » :</p> <pre><objectList type="group" select="all" resolution="merge"> <object name="Group1" resolution="reuse" /> </objectList></pre> <p>Si vous définissez un élément d'objet sans utiliser l'attribut « select », infacmd importe les objets qui satisfont les attributs définis dans l'élément d'objet. Par exemple, les lignes suivantes importent Group1 avec une stratégie de résolution « Fusionner » :</p> <pre><objectList type="group" resolution="merge"> <object name="Group1" /> </objectList></pre> <p>Si vous ne définissez pas d'élément d'objet pour objectList, la valeur par défaut de l'attribut « select » est « all ». Par exemple, les lignes suivantes importent tous les groupes avec une stratégie de résolution « Fusionner » :</p> <pre><objectList type="group" resolution="merge" /></pre> <p>La valeur valide est « all ».</p>
objectList	resolution	<p>Facultatif. Stratégie de résolution en cas de conflit de nom. S'applique à tous les objets du type spécifié. Spécifiez l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> - Remplacer. Remplace l'objet cible par l'objet source. - Renommer. Renomme l'objet source avec un nom généré, puis l'importe. Vous ne pouvez pas utiliser l'option Renommer avec le type de configuration de cluster. - Réutiliser. Réutilise l'objet dans le domaine cible. - Fusionner. Fusionne les objets en un seul objet. Cette option est applicable pour les groupes. <p>Les valeurs ne sont pas sensibles à la casse.</p>
objet	name	<p>Requis. Nom d'un objet spécifique à importer du type d'objet spécifié. La valeur n'est pas sensible à la casse.</p>

Élément	Nom de l'attribut	Description de l'attribut
objet	resolution	Facultatif. Stratégie de résolution lorsqu'un conflit de nom se produit pour cet objet. Spécifiez l'une des valeurs suivantes : <ul style="list-style-type: none"> - Remplacer. Remplace l'objet cible par l'objet source. - Renommer. Renomme l'objet source, puis l'importe. <p>Vous ne pouvez pas utiliser l'option Renommer avec le type de configuration de cluster.</p> <ul style="list-style-type: none"> - Réutiliser. Réutilise l'objet dans le domaine cible. - Fusionner. Fusionne les objets en un seul objet. Cette option est applicable pour les groupes. <p>Les valeurs ne sont pas sensibles à la casse.</p>
objet	renameTo	Facultatif. Nom à utiliser si la stratégie de résolution de conflit est « Renommer ». Si vous ne spécifiez pas de nom, infacmd en génère un en adjoignant un nombre à la fin du nom. Infacmd ignore la valeur s'il n'y a aucun conflit ou si la stratégie de résolution de conflit n'est pas « Renommer ».
objet	renamedTo	Facultatif. Chaîne d'identifiant à utiliser lorsque vous importez un objet de connexion et que la stratégie de résolution de conflit est « Renommer ». Si vous ne spécifiez pas d'identifiant de connexion, infacmd en génère un en adjoignant un nombre à la fin de l'identifiant de connexion. Infacmd ignore la valeur s'il n'y a aucun conflit ou si la stratégie de résolution de conflit n'est pas « Renommer ».

Exemple de fichier de contrôle d'importation pour les objets de domaine

Le code suivant montre un exemple de fichier de contrôle d'importation pour les objets de domaine :

```
<?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>
```

Paramètres du fichier de contrôle d'importation pour les objets du référentiel modèle

Utilisez les paramètres du fichier de contrôle d'importation pour configurer les objets que vous voulez importer dans le référentiel modèle, depuis un fichier XML.

Un fichier de contrôle d'importation pour des objets du référentiel modèle peut contenir les éléments suivants :

- importParams. Peut contenir un seul élément folderMaps et un seul élément connectionInfo.
- folderMaps. Peut contenir plusieurs éléments folderMap.
- folderMap. Contient les attributs permettant de filtrer les objets d'un dossier spécifique. Peut contenir plusieurs éléments objectList.

- **objectList.** Contient les attributs pour filtrer les objets par type. Peut contenir plusieurs éléments objet.
- **objet.** Contient les attributs pour filtrer les objets par nom.
- **connectionInfo.** Peut contenir un seul élément « **rebindMap** ».
- **rebindMap.** Peut contenir plusieurs éléments « **rebind** ».
- **rebind.** Contient des attributs pour mapper les connexions dans le référentiel source sur les connexions dans le référentiel cible.

Le tableau suivant décrit les attributs configurables pour l'élément **folderMap** dans le fichier de contrôle d'importation :

Nom d'attribut	Description de l'attribut
sourceProject	Obligatoire. Nom du projet source dans le fichier d'exportation qui contient les objets que vous voulez importer. La valeur n'est pas sensible à la casse.
sourceFolderPath	Facultatif. Chemin d'accès du dossier source dans le fichier d'exportation qui contient les objets que vous voulez importer. Utiliser le format suivant : "/<folder_name>/<folder_name>" Par exemple, si un projet contient un dossier nommé F1, le chemin d'accès du dossier F1 est « /F1 ». Pour importer tous les objets du projet, spécifiez « / ». La valeur n'est pas sensible à la casse. La valeur par défaut est « / ».
targetProject	Obligatoire. Nom du projet dans le référentiel cible dans lequel vous voulez importer des objets. Le projet doit exister dans le référentiel avant d'importer les objets. La valeur n'est pas sensible à la casse.
targetFolderPath	Facultatif. Chemin d'accès du dossier dans le référentiel cible dans lequel vous voulez importer des objets. Utiliser le format suivant : "/<folder_name>/<folder_name>" Par exemple, si un projet contient un dossier nommé F1, le chemin d'accès du dossier F1 est « /F1 ». Pour importer tous les objets dans le projet cible, spécifiez « / ». Le dossier doit exister dans le référentiel avant d'importer les objets. La valeur n'est pas sensible à la casse. La valeur par défaut est « / ».
récuratif	Facultatif. Indique si vous voulez importer les objets des sous-dossiers du dossier spécifié. Indiquez « Vrai » pour exporter à partir des sous-dossiers. Les valeurs valides sont « Vrai » et « Faux ». Cette valeur est sensible à la casse. La valeur par défaut est True.

Nom d'attribut	Description de l'attribut
select	<p>Facultatif. Indique si infacmd importe tous les objets restants du projet spécifié lorsque vous définissez un élément objectList pour folderMap. Définir « Tous » pour importer tous les objets restants. Par exemple, les lignes suivantes importent les mappages avec une stratégie de résolution « Réutiliser ». Les lignes importent tous les objets restants avec une stratégie de résolution « Remplacer » :</p> <pre><folderMap sourceProject="p1" targetProject="p2" select="all" resolution="replace"> <objectList type="Mapping" resolution="reuse" /> </folderMap></pre> <p>Si vous définissez un élément objectList sans utiliser l'attribut « Sélectionner », infacmd importe les objets qui satisfont les attributs définis dans objectList. Par exemple, les lignes suivantes importent les mappages avec une stratégie de résolution « Remplacer » :</p> <pre><folderMap sourceProject="p1" targetProject="p2" resolution="replace"> <objectList type="Mapping" /> </folderMap></pre> <p>Si vous ne définissez pas d'élément objectList pour folderMap, la valeur par défaut est « Tous ». Par exemple, la ligne suivante importe tous les objets avec une stratégie de résolution « Remplacer » :</p> <pre><folderMap sourceProject="p1" targetProject="p2" resolution="replace" /></pre> <p>La valeur valide est « Tous ».</p>
resolution	<p>Facultatif. Stratégie de résolution en cas de conflit de nom. S'applique à tous les objets du dossier. Spécifiez une des valeurs suivantes :</p> <ul style="list-style-type: none"> - Renommer. Renommer l'objet source avec un nom généré, puis l'importer. - Remplacer. Remplacer l'objet cible par l'objet source. - Réutiliser. Réutiliser l'objet dans le référentiel modèle cible. - Aucun. <p>Les valeurs ne sont pas sensibles à la casse. La valeur par défaut est « Aucun ».</p>

Le tableau suivant décrit les attributs configurables pour l'élément `objectList` dans le fichier de contrôle d'importation :

Nom d'attribut	Description de l'attribut
type	Obligatoire. Type d'objet du référentiel modèle à importer dans le chemin de dossier spécifié. Les valeurs valides comprennent tous les types d'objets présents dans le référentiel modèle. Vous pouvez afficher le type de l'objet dans la vue Propriétés de l'outil Developer. Par exemple, vous pouvez entrer « Objet de données relationnel » ou « Profil ». La valeur n'est pas sensible à la casse.
select	<p>Facultatif. Indique si infacmd importe tous les objets restants du type spécifié lorsque vous définissez un élément d'objet pour <code>objectList</code>. Définir « Tous » pour importer tous les objets restants. Par exemple, les lignes suivantes importent MyMapping avec une résolution de stratégie « Réutiliser ». Les lignes importent tous les mappages restants avec une stratégie de résolution « Remplacer » :</p> <pre><folderMap sourceProject="p1" targetProject="p2"> <objectList type="Mapping" select="all" resolution="replace"> <object name="MyMapping" resolution="reuse" /> </objectList> </folderMap></pre> <p>Si vous définissez un élément d'objet sans utiliser l'attribut « Sélectionner », infacmd importe les objets qui satisfont les attributs définis dans l'élément d'objet. Par exemple, les lignes suivantes importent le mappage nommé MyMapping avec une stratégie de résolution « Remplacer » :</p> <pre><folderMap sourceProject="p1" targetProject="p2"> <objectList type="Mapping" resolution="replace"> <object name="MyMapping"/> </objectList> </folderMap></pre> <p>Si vous ne définissez pas d'élément d'objet pour <code>objectList</code>, la valeur par défaut est « Tous ». Par exemple, les lignes suivantes importent tous les mappages avec une stratégie de résolution « Remplacer » :</p> <pre><folderMap sourceProject="p1" targetProject="p2"> <objectList type="Mapping" resolution="replace" /> </folderMap></pre> <p>La valeur valide est « Tous ».</p>
resolution	<p>Facultatif. Stratégie de résolution en cas de conflit de nom. S'applique à tous les objets du type spécifié. Spécifiez une des valeurs suivantes :</p> <ul style="list-style-type: none"> - Renommer. Renommer l'objet source avec un nom généré, puis l'importer. - Remplacer. Remplacer l'objet cible par l'objet source. - Réutiliser. Réutiliser l'objet dans le référentiel modèle cible. - Aucun. <p>Les valeurs ne sont pas sensibles à la casse. La valeur par défaut est « Aucun ».</p>

Le tableau suivant décrit les attributs configurables pour l'élément d'objet dans le fichier de contrôle d'importation :

Nom d'attribut	Description de l'attribut
name	Obligatoire. Nom d'un objet spécifique à importer du type d'objet spécifié. La valeur n'est pas sensible à la casse.
resolution	Facultatif. Stratégie de résolution lorsqu'un conflit de nom se produit pour cet objet. Spécifiez une des valeurs suivantes : <ul style="list-style-type: none"> - Renommer. Renommer l'objet source, puis l'importer. - Remplacer. Remplacer l'objet cible par l'objet source. - Réutiliser. Réutiliser l'objet dans le référentiel modèle cible. - Aucun. Les valeurs ne sont pas sensibles à la casse. La valeur par défaut est « Aucun ».
renameTo	Facultatif. Nom à utiliser si la stratégie de résolution de conflit est « Renommer ». Si vous ne spécifiez pas de nom, infacmd en génère un en adjoignant un nombre à la fin du nom. Infacmd ignore la valeur s'il n'y a aucun conflit ou si la stratégie de résolution de conflit n'est pas « Renommer ».
renameIdTo	Facultatif. Chaîne d'identifiant à utiliser lorsque vous importez un objet de connexion et lorsque la stratégie de résolution de conflit est « Renommer ». Si vous ne spécifiez pas d'identifiant de connexion, infacmd générera alors un identifiant en ajoutant un nombre à la fin de l'identifiant de connexion. Infacmd ignore la valeur s'il n'y a aucun conflit ou si la stratégie de résolution de conflit n'est pas « Renommer ».

Le tableau suivant décrit les attributs configurables pour l'élément « rebind » dans le fichier de contrôle d'importation :

Nom d'attribut	Description de l'attribut
source	Obligatoire. Nom d'une connexion source dans le fichier en cours d'importation. La valeur n'est pas sensible à la casse.
cible	Obligatoire. Nom d'une connexion dans le référentiel modèle cible à mapper sur la connexion source. Par défaut, la connexion doit exister dans le référentiel cible avant de procéder à l'importation des objets. L'importation échoue si la connexion n'existe pas. Lorsque vous exécutez la commande infacmd, vous pouvez choisir d'ignorer la validation de connexion cible pendant l'importation. Lorsque vous ignorez la validation de connexion, l'importation aboutit si aucune connexion n'existe dans le référentiel cible. La valeur n'est pas sensible à la casse.

Exemple du fichier de contrôle d'importation pour les objets du référentiel modèle

Le code suivant montre un exemple de fichier de contrôle d'importation pour les objets du référentiel modèle :

```
<?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>

<!-- 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>

```

Règles et directives concernant les fichiers de contrôle

Consultez les règles et directives suivantes avant de créer des fichiers de contrôle :

- Les noms de l'élément et de l'attribut sont sensibles à la casse.
- Les fichiers de contrôle contiennent une hiérarchie d'éléments XML. Les éléments à des niveaux différents peuvent contenir le même attribut. Un élément enfant dont la valeur d'attribut n'est pas définie hérite de la valeur du même attribut de l'élément parent. Quand la valeur d'attribut de l'élément enfant est définie, elle écrase la valeur du même attribut de l'élément parent.
- Quand un élément définit plusieurs attributs, infacmd exporte ou importe les objets qui correspondent à tous les attributs de filtres. Par exemple, vous définissez les attributs `createdBefore` et `lastUpdatedAfter` pour un élément `objectList` dans un fichier de contrôle d'exportation. Infacmd exporte les objets du type spécifié créés avant la date spécifiée et dont la dernière mise à jour a été réalisée après la date spécifiée.
- Les valeurs des attributs « time » ne sont pas inclusives. Par exemple, vous définissez `createdAfter` avec « 2011-02-01 16:00:00-0800 » dans un fichier de contrôle d'exportation. Infacmd exporte tous les objets créés après 16 h le 1er février 2011. Les objets créés à 16 h le 1er février 2011 ne sont pas exportés par infacmd.
- Vous ne pouvez spécifier qu'un seul `objectList` d'un type spécifique dans un fichier de contrôle pour les objets du domaine. Par exemple, vous spécifiez un `objectList` dont le type est « connexion ». Vous ne pouvez pas spécifier un autre `ObjectList` de type « connexion » dans le même fichier.
- Vous ne pouvez spécifier qu'un seul `objectList` d'un type spécifique dans un dossier ou dans un élément `folderMap` pour les objets du référentiel modèle. Par exemple, vous spécifiez un `objectList` dont le type est « Flat File Data Object ». Vous ne pouvez pas spécifier un autre `ObjectList` de type « Flat File Data Object » dans le même dossier ou le même élément `folderMap`.

Exemples de fichier de contrôle pour les objets de domaine

Vous pouvez filtrer les objets de domaine pour les exporter en fonction de l'heure. Vous pouvez filtrer les objets de domaine pour les exporter et les importer en fonction du type d'objet ou du nom d'objet.

Exporter les objets de domaine par heure

Pour exporter les utilisateurs créés après 2010-12-25 10:00:00 + 0530, vous pouvez créer le fichier de contrôle suivant :

```
<?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>
```

Exporter et importer les objets de domaine par type

Pour exporter depuis un domaine tous les utilisateurs, les groupes et les rôles en filtrant les connexions, vous pouvez créer le fichier de contrôle suivant :

```
<?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>
```

Pour importer dans un domaine tous les utilisateurs et tous les groupes en filtrant les rôles et les connexions, vous pouvez créer le fichier de contrôle suivant :

```
<?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>
```

Exporter et importer les objets de domaine par nom

Vous voulez exporter tous les utilisateurs et tous les groupes ainsi que les rôles Developer et Analyst depuis le domaine source. Vous voulez exporter des connexions spécifiques créées après 2011-02-01 16:00:00-0800. Vous pouvez créer le fichier de contrôle suivant :

```
<?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>
```

Pour importer dans le domaine cible tous les utilisateurs et tous les groupes, ainsi que des rôles et des connexions spécifiques, vous pouvez créer le fichier de contrôle suivant :

```
<?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" />
  </objectList>
</importParams>
```

```

    <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>

```

Exemples de fichier de contrôle pour les objets du référentiel modèle

Vous pouvez filtrer l'exportation d'objets du référentiel modèle par heure ou par utilisateur. Vous pouvez filtrer l'exportation ou l'importation d'objets du référentiel modèle par type d'objet ou par nom d'objet.

Exportation d'objets du référentiel modèle par heure

Pour exporter tous les objets d'un dossier nommé Dossier1 créé avant 2011-02-01 16:00:00-0800, vous pouvez créer le fichier de contrôle suivant :

```

<?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>

```

Exportation d'objets du référentiel modèle par utilisateur

Pour exporter tous les objets du projet dont la dernière mise à jour a été effectuée par l'administrateur, vous pouvez créer le fichier de contrôle suivant :

```

<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
  <folders>
    <folder lastUpdatedBy="Administrator" />
  </folders>
</exportParams>

```

Exporter et importer les objets du référentiel modèle par type

Pour exporter tous les mappages d'un dossier nommé Dossier1, vous pouvez créer le fichier de contrôle suivant :

```

<?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>

```

Vous voulez exporter tous les mappages créés par user2 et exporter tous les objets restants créés par user1. L'attribut createdBy défini pour l'élément enfant ObjectList écrase le même attribut défini pour l'élément du dossier parent. Vous pouvez créer le fichier de contrôle suivant :

```

<?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>

```

```

</folders>
</exportParams>

```

Vous voulez importer tous les mappages du fichier d'exportation. Certains des mappages exportés depuis Dossier1 contiennent des objets dépendants qui existaient dans Dossier2 dans le référentiel source. Pour importer des objets dépendants, vous devez inclure tous les objets dépendants à l'aide des éléments `folderMap` dans le fichier de contrôle d'importation. Vous voulez aussi mapper les connexions dans le référentiel source sur les connexions du référentiel cible. Vous pouvez créer le fichier de contrôle suivant :

```

<?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>

```

Exporter et importer des objets du référentiel modèle par nom

Vous voulez exporter un mappage nommé `TestMapping` créé après 2010-11-11 23:59:59-0800. Vous voulez exporter tous les objets restants dans le même dossier. Vous pouvez créer le fichier de contrôle suivant :

```

<?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>

```

Un fichier d'exportation contient des objets de fichier plat et de données relationnelles. Vous voulez importer l'objet de données du fichier plat nommé `NewFlatFileDataObject` et tous les objets de données relationnelles depuis le fichier d'exportation. Vous pouvez créer le fichier de contrôle suivant :

```

<?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>

```

CHAPITRE 42

Référence de commande infasetup

Ce chapitre comprend les rubriques suivantes :

- [Utilisation d'infasetup, 1274](#)
- [BackupDomain, 1275](#)
- [DefineDomain, 1278](#)
- [DefineGatewayNode, 1288](#)
- [DefineWorkerNode, 1294](#)
- [DeleteDomain, 1298](#)
- [GenerateEncryptionKey, 1301](#)
- [Aide, 1301](#)
- [ListDomainCiphers, 1302](#)
- [MigrateEncryptionKey, 1303](#)
- [RestoreDomain, 1303](#)
- [restoreMitKerberosLinkage, 1306](#)
- [SwitchToKerberosMode, 1307](#)
- [UpdateDomainCiphers, 1308](#)
- [updateDomainName, 1311](#)
- [UpdateGatewayNode, 1311](#)
- [UpdateKerberosAdminUser, 1317](#)
- [UpdateKerberosConfig, 1317](#)
- [updateMitKerberosLinkage, 1318](#)
- [UpdatePasswordComplexityConfig, 1319](#)
- [UpdateDomainSamlConfig, 1320](#)
- [UpdateWorkerNode, 1323](#)
- [upgradeDomainMetadata, 1328](#)
- [UpgradeGatewayNodeMetadata, 1329](#)
- [UnlockUser, 1331](#)
- [ValidateandRegisterFeature, 1332](#)

Utilisation d'infasetup

infasetup est un programme de ligne de commande que vous utilisez pour gérer des domaines et des nœuds Informatica.

Utilisez *infasetup* pour modifier les propriétés de domaine et de nœud après avoir installé les services Informatica à l'aide du programme d'installation Informatica. Par exemple, vous pouvez utiliser *infasetup* pour changer le numéro de port d'un nœud après avoir installé les services Informatica.

Vous pouvez utiliser *infasetup* pour sauvegarder, restaurer, définir et supprimer des domaines et pour définir et mettre à jour des nœuds.

Exécution de commandes

Vous devez appeler *infasetup* avec la ligne de commande. Vous pouvez exécuter les commandes directement ou à partir d'un script, un fichier de lots ou d'autres programme. Sous Windows, *infasetup* est un fichier de lots avec une extension « .bat ». Sous UNIX, *infasetup* est un fichier de script avec une extension « .sh ».

Pour exécuter des commandes *infasetup* :

1. Ouvrez une invite de commande.

Sous Windows, ouvrez l'invite de commande en tant qu'administrateur. Si vous n'ouvrez pas l'invite de commande en tant qu'administrateur, l'administrateur système Windows peut rencontrer des problèmes lors de l'accès aux fichiers dans le répertoire d'installation d'Informatica.

2. À l'invite de commande, passez au répertoire abritant l'exécutable *infasetup*.

Par défaut, *infasetup* s'installe dans le répertoire <InformaticaInstallationDir>/isp/bin.

3. Saisissez *infasetup* sous Windows ou *infasetup.sh* sous UNIX suivi du nom de la commande et les options et arguments obligatoires. Les noms de commandes ne sont pas sensibles à la casse.

Par exemple :

```
infasetup(.sh) command_name [-option1] argument_1 [-option2] argument_2...
```

Options de commande

Lorsque vous exécutez la commande *infacmd*, vous saisissez des options pour chaque commande, suivies par les arguments obligatoires. Les options de commande sont précédées par un trait d'union et ne sont pas sensibles à la casse. Les arguments suivent l'option.

Par exemple, la commande suivante met à jour un nœud de travail dont le nom est « Node1 » et l'adresse, « Host1:9090 » :

```
infasetup UpdateWorkerNode -nn Node1 -na Host1:9090
```

Si vous omettez ou saisissez de manière incorrecte l'une des options obligatoires, la commande échoue et *infasetup* renvoie un message d'erreur.

Codes de retour infasetup

infacmd indique la réussite ou l'échec d'une commande à l'aide d'un code de retour. Code de retour (0) indique que la commande a réussi. Code de retour (-1) indique que la commande a échoué.

Utilisez la commande DOS ou UNIX « echo » immédiatement après avoir exécuté une commande *infasetup* pour voir le code de retour de cette commande :

- Dans un shell DOS : `echo %ERRORLEVEL%`
- Dans un shell UNIX Bourne ou Korn : `echo $?`
- Dans un shell C UNIX : `echo $status`

Utilisation des chaînes de connexion à la base de données

Certaines commandes *infasetup* utilisent des chaînes de connexion pour se connecter à la base de données de configuration du domaine. Spécifiez l'hôte de la base de données, le port de la base de données et le nom du service de base de données en tant qu'éléments de la chaîne de connexion.

Vous pouvez utiliser des chaînes de connexion avec les commandes *infasetup* suivantes :

- BackupDomain
- DefineDomain
- DefineGatewayNode
- DeleteDomain
- RestoreDomain
- UpdateGatewayNode

Le tableau suivant répertorie la syntaxe de chaîne de connexion pour chaque base de données prise en charge :

Nom de la base de données	Chaîne de connexion
Oracle	Oracle : <code>jdbc:informatica:oracle://host_name:port;SID=sid</code> Oracle RAC : <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

Sauvegarde les métadonnées de configuration du domaine. *infasetup* stocke les métadonnées du domaine de sauvegarde dans un fichier de sauvegarde portant l'extension `.mrep`.

Vous devez arrêter le domaine avant d'exécuter cette commande.

Lorsque vous exécutez cette commande, *infasetup* sauvegarde les tables de base de données de configuration de domaine pour restaurer le domaine dans une autre base de données. Vous devez sauvegarder manuellement le contenu de la table `ISP_RUN_LOG` pour obtenir le flux de travail précédent et les journaux de session.

Si la commande échoue en indiquant une erreur de mémoire Java, augmentez la mémoire système allouée à la commande `infasetup`. Pour augmenter la mémoire système, définissez la valeur `-Xmx` dans la variable d'environnement `INFA_JAVA_CMD_OPTS`.

La commande `BackupDomain` utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'*infasetup* `BackupDomain` :

Option	Argument	Description
-DatabaseAddress -da	database_hostname:database_port	Requis si vous n'utilisez pas l'option -DatabaseConnectionString (-cs). Nom et numéro du port de la machine hébergeant la base de données de configuration du domaine.
-DatabaseConnectionString -cs	database_connection_string	Requis si vous n'utilisez pas les options -DatabaseAddress (-da) et -DatabaseServiceName (-ds). Chaîne de connexion utilisée pour se connecter à la base de données de configuration du domaine. La chaîne de connexion doit inclure l'hôte de la base de données, le port de la base de données et le nom du service de base de données. Placez la chaîne de connexion entre guillemets.
-DatabaseUserName -du	database_user_name	Requis si vous n'utilisez pas l'option -TrustedConnection (-tc). Compte de la base de données qui contient les informations de configuration du domaine.

Option	Argument	Description
-DatabasePassword -dp	database_password	Mot de passe de la base de données de configuration du domaine correspondant à l'utilisateur de la base de données. Si vous omettez cette option, <i>infasetup</i> utilisera le mot de passe spécifié dans la variable d'environnement INFA_DEFAULT_DATABASE_PASSWORD. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, vous devez entrer un mot de passe à l'aide de cette option.
-DatabaseType -dt	database_type	Requis. Type de base de données contenant les métadonnées de configuration du domaine. Les types de base de données sont les suivants : - db2 - oracle - mssqlserver - sybase
-DatabaseServiceName -ds	database_service_name	Requis si vous n'utilisez pas l'option - DatabaseConnectionString (-cs). Nom du service de base de données. Requis pour les bases de données Oracle, IBM DB2 et Microsoft SQL Server. Entrez le SID pour Oracle, le nom du service pour IBM DB2 ou le nom de la base de données pour Microsoft SQL Server.
-BackupFile -bf	backup_file_name	Requis. Nom et chemin du fichier de sauvegarde. Si vous ne spécifiez pas de chemin de fichier, <i>infasetup</i> crée le fichier de sauvegarde dans le répertoire actuel.
-Force -f	-	Facultatif. Remplace le fichier de sauvegarde si un fichier du même nom existe déjà.
-DomainName -dn	domain_name	Requis. Nom du domaine.
-Tablespace -ts	tablespace_name	Requis dans le cas d'une base de données IBM DB2. Nom de l'espace de table dans lequel se situent les tables de la base de données de configuration du domaine.
-SchemaName -sc	schema_name	Facultatif. Nom du schéma Microsoft SQL Server. Entrez un nom de schéma si vous n'utilisez pas le schéma par défaut.
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Facultatif. Indique si la base de données du domaine Informatica est sécurisée avec le protocole TLS ou SSL. Définissez cette option sur True pour la base de données sécurisée. La valeur par défaut est false. Si vous spécifiez l'option -dbtls sans valeur, le domaine Informatica utilise la communication sécurisée avec la base de données du domaine Informatica.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Facultatif. Mot de passe du fichier truststore de la base de données sécurisée.

Option	Argument	Description
-TrustedConnection -tc	-	Facultatif. Connexion à la base de données Microsoft SQL Server via une connexion approuvée. L'authentification de confiance utilise les justificatifs d'identité de sécurité Windows de l'utilisateur en cours pour effectuer la connexion à Microsoft SQL Server.
-EncryptionKeyLocation -kl	encryption_key_location	Facultatif. Répertoire contenant la clé de cryptage actuelle. Vous devez spécifier l'emplacement de la clé si la clé de chiffrement n'existe pas dans le fichier isp/config/nodemeta.xml. Le nom du fichier de cryptage est sitekey.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Chemin et nom du fichier truststore de la base de données du référentiel de domaine sécurisé. Requis si vous configurez une base de données du référentiel de domaine sécurisé pour le domaine.

DefineDomain

Crée un domaine sur la machine actuelle. Si vous définissez un domaine sur une machine hébergeant un domaine, vous devez d'abord arrêter les services Informatica sur la machine. La commande infasetup supprime le domaine existant et les paramètres des nœuds. Après avoir défini le nouveau domaine, redémarrez les services Informatica.

Pour créer un domaine dans un environnement Windows, vous devez en premier lieu ouvrir le port hôte ou désactiver le pare-feu.

Aucun caractère ne doit figurer après l'option (-f) dans la commande DefineDomain. Si vous incluez des caractères supplémentaires, la commande peut échouer avec une erreur inattendue.

La commande DefineDomain utilise la syntaxe suivante :

```
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|-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]
[<-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]

```

Le tableau suivant décrit les options et arguments de la commande `infasetup DefineDomain` :

Option	Description
-DatabaseAddress -da	Obligatoire si vous n'utilisez pas l'option -DatabaseConnectionString (-cs). Nom et numéro du port de la machine hébergeant la base de données de configuration du domaine.
-DatabaseConnectionString -cs	Obligatoire si vous n'utilisez pas les options -DatabaseAddress (-da) et --DatabaseServiceName (-ds). Chaîne de connexion utilisée pour se connecter à la base de données de configuration du domaine. La chaîne de connexion doit inclure l'hôte de la base de données, le port de la base de données et le nom du service de base de données. Placez la chaîne de connexion entre guillemets.
-DatabaseUserName -du	Obligatoire si vous n'utilisez pas l'option -TrustedConnection (-tc). Compte de la base de données qui contient les informations de configuration du domaine.
-DatabasePassword -dp	Mot de passe de la base de données de configuration du domaine correspondant à l'utilisateur de la base de données. Si vous omettez cette option, <i>infasetup</i> utilisera le mot de passe spécifié dans la variable d'environnement <code>INFA_DEFAULT_DATABASE_PASSWORD</code> . Si vous ne voyez pas une valeur spécifiée dans la variable d'environnement, vous devez entrer un mot de passe à l'aide de cette option.
-DatabaseType -dt	Requis. Type de base de données contenant les métadonnées de configuration du domaine. Les types de base de données sont les suivants : <ul style="list-style-type: none"> - db2 - oracle - mssqlserver - sybase - postgresql
-DatabaseServiceName -ds	Obligatoire si vous n'utilisez pas l'option -DatabaseConnectionString (-cs). Nom du service de base de données. Obligatoire pour les bases de données Oracle, IBM DB2 et Microsoft SQL Server. Entrez le SID pour Oracle, le nom du service pour IBM DB2 ou le nom de la base de données pour Microsoft SQL Server.
-Tablespace -ts	Obligatoire dans le cas d'une base de données IBM DB2. Nom de l'espace de table dans lequel se situent les tables de la base de données de configuration du domaine.
-SchemaName -sc	Facultatif. Nom du schéma Microsoft SQL Server ou PostgreSQL. Entrez un nom de schéma si vous n'utilisez pas le schéma par défaut.
-DatabaseTlsEnabled -dbtls	Facultatif. Indique si la base de données du domaine Informatica est sécurisée avec le protocole TLS ou SSL. Définissez cette option sur True pour la base de données sécurisée. La valeur par défaut est False. Si vous spécifiez l'option -dbtls sans valeur, le domaine Informatica utilise la communication sécurisée avec la base de données du domaine Informatica.
-DatabaseTruststorePassword -dbtp	Facultatif. Mot de passe du fichier truststore de la base de données sécurisée.

Option	Description
-DomainName -dn	Requis. Nom du domaine. Les noms de domaine doivent avoir une longueur comprise entre 1 et 79 caractères et ne peuvent contenir ni des espaces, ni les caractères suivants : / * ? < > "
-DomainDescription -de	Facultatif. Description du domaine.
-AdministratorName -ad	Requis. Nom de l'administrateur du domaine. Si un domaine Kerberos unique est utilisé pour authentifier les utilisateurs, spécifiez le nom samAccount. Si le domaine utilise l'authentification Kerberos inter-domaines, spécifiez le nom du principal de l'utilisateur complet, y compris le nom du domaine. Par exemple : sysadmin@COMPANY.COM
-Password -pd	Facultatif pour le domaine Kerberos. Mot de passe administrateur du domaine. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire. Pour un compte utilisateur natif, si vous activez la complexité du mot de passe, utilisez les directives suivantes lorsque vous créez ou modifiez un mot de passe : - Le mot de passe doit contenir au moins huit caractères. - Il doit être composé d'un caractère alphabétique, d'un caractère numérique et d'un caractère non alphanumérique, tels que : ! \ " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { } ~ Lorsque vous utilisez des caractères spéciaux dans un mot de passe, il arrive que l'interpréteur de commandes les lise différemment. Par exemple, \$ est interprété comme une variable. Dans ce cas, utilisez un caractère d'échappement pour échapper le caractère spécial.
-LicenseName -ln	Facultatif. Nom de la licence. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Le nom ne peut pas dépasser 79 caractères, commencer ou terminer par des espaces ou encore contenir des retours à la ligne, des tabulations ou les caractères suivants : / * ? < > "
-LicenseKeyFile -lf	Facultatif. Chemin du fichier de clé de licence.
-LogServiceDirectory -ld	Requis. Chemin du répertoire partagé utilisé par le gestionnaire de journaux pour stocker des fichiers d'événements de journal. Vérifiez que -ld ne correspond pas à la valeur--sld spécifiée ni ne la contient.
-SystemLogDirectory -sld	Facultatif. Chemin du répertoire pour stocker les fichiers journaux système. Vérifiez que -ld ne correspond pas à la valeur--sld spécifiée ni ne la contient. La valeur par défaut est <INFA_home>/logs.
-NodeName -nn	Requis. Nom du nœud. Les noms de nœud doivent avoir une longueur comprise entre 1 et 79 caractères et ne peuvent contenir ni des espaces, ni les caractères suivants : \ / * ? < > "

Option	Description
-NodeAddress -na	Requis. Nom d'hôte et numéro de port de la machine hébergeant le nœud. Choisissez un numéro de port disponible.
-ServiceManagerPort -sp	Facultatif. Numéro de port utilisé par le gestionnaire de service pour écouter les demandes de connexions entrantes.
-EnableTLS -tls	Facultatif. Configure la communication sécurisée des services dans le domaine Informatica. Si vous utilisez les certificats SSL par défaut fournis par Informatica, vous n'avez pas besoin de spécifier les options keystore et truststore. Si vous n'utilisez pas le certificat SSL par défaut, vous devez spécifier les options keystore et truststore. Les valeurs valides sont True ou False. La valeur par défaut est False. Si vous spécifiez l'option -tls sans valeur, le domaine Informatica utilise la communication sécurisée entre les services. Pour activer la communication sécurisée pour les services ou applications Web associés, tels que l'outil Administrator tool, l'outil Analyst tool ou le hub de services Web, configurez la communication sécurisée séparément dans les applications.
-NodeKeystore- -nk	Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Obligatoire si vous utilisez vos certificats SSL. Répertoire contenant les fichiers keystore. Le domaine Informatica requiert les certificats SSL au format PEM et dans des fichiers Java Keystore (JKS). Le répertoire doit contenir les fichiers keystore aux formats PEM et JKS. Les fichiers keystore doivent être nommés infa_keystore.jks et infa_keystore.pem. Si le fichier keystore que vous recevez de l'autorité de certification (CA) a un nom différent, vous devez le renommer infa_keystore.jks et infa_keystore.pem. Vous devez utiliser le même fichier keystore pour tous les nœuds du domaine.
-NodeKeystorePass -nkp	Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Obligatoire si vous utilisez vos certificats SSL. Mot de passe pour le fichier keystore infa_keystore.jks.
-NodeTruststore -nt	Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Répertoire contenant les fichiers truststore. Le domaine Informatica requiert les certificats SSL au format PEM et dans des fichiers Java Keystore (JKS). Le répertoire doit contenir les fichiers truststore aux formats PEM et JKS. Les fichiers truststore doivent être nommés infa_truststore.jks et infa_truststore.pem. Si le fichier truststore que vous recevez de l'autorité de certification (CA) a un nom différent, vous devez le renommer infa_truststore.jks et infa_truststore.pem.
-NodeTruststorePass -ntp	Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Requis si vous utilisez vos certificats SSL. Mot de passe du fichier infa_truststore.jks.
-CipherWhiteList -cwl	Facultatif. Liste séparée par des virgules de suites de chiffrement JSSE que vous souhaitez ajouter à la liste effective. Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.

Option	Description
-CipherBlackList -cbl	Facultatif. Liste séparée par des virgules de suites de chiffrement JSSE que vous souhaitez supprimer de la liste effective. Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.
-CipherWhiteListFile -cwlf	Facultatif. Nom de fichier absolu du fichier en texte brut qui contient une liste de suites de chiffrement séparée par des virgules à ajouter à la liste effective. Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.
-CipherBlackListFile -cblf	Facultatif. Nom de fichier absolu du fichier en texte brut qui contient une liste de suites de chiffrement séparée par des virgules que vous souhaitez supprimer de la liste effective. Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.
-EnableKerberos -krb	Facultatif. Configure le domaine Informatica pour qu'il utilise l'authentification Kerberos. Les valeurs valides sont True ou False. Si la valeur est True, le domaine utilise l'authentification Kerberos et vous ne pouvez plus changer le mode d'authentification. Après avoir activé l'authentification Kerberos, vous ne pouvez pas la désactiver. La valeur par défaut est False. Si vous spécifiez l'option -krb sans valeur, le domaine Informatica utilise l'authentification Kerberos.
-ServiceRealmName -srn	Facultatif. Nom du domaine Kerberos utilisé pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules. Pour configurer l'authentification Kerberos inter-domaines, spécifiez le nom de chaque domaine Kerberos utilisé pour l'authentification des utilisateurs, séparé par une virgule. Par exemple : COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple, spécifiez la valeur suivante afin d'inclure tous les domaines qui incluent le nom EAST.COMPANY.COM : *EAST.COMPANY.COM
-UserRealmName -urn	Facultatif. Nom du domaine Kerberos utilisé pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules. Pour configurer l'authentification Kerberos inter-domaines, spécifiez le nom de chaque domaine Kerberos utilisé pour l'authentification des utilisateurs, séparé par une virgule. Par exemple : COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple, spécifiez la valeur suivante afin d'inclure tous les domaines qui incluent le nom EAST.COMPANY.COM : *EAST.COMPANY.COM
-KeysDirectory -kd	Facultatif. Répertoire dans lequel sont stockés tous les fichiers Keytab et la clé de cryptage pour le domaine Informatica. La valeur par défaut est <Informatica installation directory>/isp/config/keys.

Option	Description
-SPNShareLevel -spnSL	Facultatif. Indique le niveau du principal du service du domaine. Définissez la propriété sur l'un des niveaux suivants : <ul style="list-style-type: none"> - Processus. Le domaine requiert un nom unique de principal du service (SPN) et un fichier Keytab pour chaque nœud et chaque service sur ce nœud. Le nombre de SPN et de fichiers Keytab requis pour chaque nœud dépend du nombre de processus de service exécutés sur le nœud. Utilisez l'option de niveau nœud si le domaine ne nécessite pas un niveau élevé de sécurité. - Nœud. Le domaine utilise un SPN et un fichier Keytab pour le nœud et tous les services exécutés sur celui-ci. Il requiert également un SPN et un fichier Keytab distincts pour tous les processus HTTP sur le nœud. La valeur par défaut est le processus.
-EnableSaml -saml	Facultatif. Active ou désactive l'authentification SAML dans le domaine Informatica. Définissez cette valeur sur True pour activer l'authentification SAML dans le domaine Informatica. La valeur par défaut est False.
-idpUrl -iu	Obligatoire si l'option -saml est définie sur true. Spécifiez l'URL du fournisseur d'identité SAML.
-ServiceProviderId -spid	Facultatif. Nom d'approbation de la partie de confiance ou identificateur de fournisseur de services pour le domaine, tel que défini dans le fournisseur d'identité. Si vous avez spécifié « Informatica » comme nom de tiers de confiance dans AD FS, vous n'avez pas besoin de spécifier une valeur.
-ClockSkewTolerance -cst	Facultatif. Différence temporelle autorisée entre l'horloge système de l'hôte du fournisseur d'identité et celle du nœud principal de passerelle. La durée de vie des jetons SAML émis par le fournisseur d'identité est définie selon l'horloge système de l'hôte du fournisseur d'identité. La durée de vie d'un jeton SAML émis par le fournisseur d'identité est valide si l'heure de début ou l'heure de fin définie dans le jeton est comprise dans le nombre de secondes spécifié de l'horloge système du nœud principal de passerelle. Les valeurs doivent être comprises entre 0 et 600 secondes. La valeur par défaut est 120 secondes.
-SamlAssertionSigned -sas	Facultatif. Définissez cette option sur TRUE pour activer la signature d'assertion par le fournisseur d'identité. La valeur par défaut est FALSE.
-AssertionSigningCertificateAlias -asca	Obligatoire si SamlAssertionSigned est défini sur TRUE. Nom d'alias spécifié lors de l'importation du certificat de signature d'assertion du fournisseur d'identité dans le fichier truststore utilisé pour l'authentification SAML.
-SamlTrustStoreDir -std	Facultatif. Répertoire contenant le fichier truststore personnalisé requis pour utiliser l'authentification SAML sur les nœuds de passerelle dans le domaine. Spécifiez le répertoire uniquement, pas le chemin d'accès complet au fichier. La valeur par défaut du fichier truststore d'Informatica est utilisée si aucun fichier truststore n'est spécifié.
-SamlTrustStorePassword -stp	Obligatoire si vous utilisez un fichier truststore personnalisé pour l'authentification SAML. Mot de passe du fichier truststore personnalisé.

Option	Description
-SamlKeyStoreDir -skd	Facultatif. Répertoire contenant le fichier keystore personnalisé requis pour utiliser l'authentification SAML sur le nœud de passerelle. Spécifiez le répertoire uniquement, pas le chemin d'accès complet au fichier.
-SamlKeyStorePassword -skp	Obligatoire si vous utilisez un fichier keystore personnalisé pour l'authentification SAML. Mot de passe du keystore SAML. *
-AuthnContextComparsion -acc	Spécifie la méthode de comparaison utilisée pour évaluer l'instruction d'autorisation demandée. Un des éléments suivants : <ul style="list-style-type: none"> - MINIMUM. Le contexte d'authentification dans l'instruction d'authentification doit correspondre exactement à au moins un des contextes d'authentification spécifiés. - MAXIMUM. Le contexte d'authentification dans l'instruction d'authentification doit être au moins aussi fort (tel que jugé par le répondeur) que l'un des contextes d'authentification spécifiés. - BETTER. Le contexte d'authentification dans l'instruction d'authentification doit être plus fort (tel que jugé par le répondeur) que l'un des contextes d'authentification spécifiés. - EXACT. Le contexte d'authentification dans l'instruction d'authentification doit être aussi fort que possible (tel que jugé par le répondeur), sans dépasser la force d'au moins un des contextes d'authentification spécifiés. La valeur par défaut est Exact.
-AuthnContextClassRef -accr	Classe du contexte d'authentification. Un des suivants : <ul style="list-style-type: none"> - PASSWORD - PASSWORDPROTECTEDTRANSPORT
-SignSamlRequest -ssr	Défini sur True pour activer la demande signée. La valeur par défaut est False.
-RequestSigningPrivateKeyAlias -rspa	Requis si vous activez la demande signée. Nom d'alias de la clé privée présente dans le keystore SAML du nœud à l'aide de laquelle la demande SAML doit être signée
-RequestSigningPrivateKeyPassword -rpp	Requis si vous activez la demande signée. Mot de passe permettant d'accéder à la clé privée utilisée pour la signature de la demande SAML
-RequestSigningAlgorithm -rsa	Requis si vous activez la demande signée. Algorithme utilisé pour signer la demande. Un des suivants : <ul style="list-style-type: none"> - RSA_SHA256 - DSA_SHA1 - DSA_SHA256 - RSA_SHA1 - RSA_SHA224 - RSA_SHA384 - RSA_SHA512 - ECDSA_SHA1 - ECDSA_SHA224 - ECDSA_SHA256 - ECDSA_SHA384 - ECDSA_SHA512 - RIPEMD160 - RSA_MD5

Option	Description
-SamlResponseSigned -srs	Défini sur True pour activer la réponse signée. La valeur par défaut est False.
-ResponseSigningCertificateAlias -rsca	Requis si vous activez la réponse signée. Nom d'alias du certificat présent dans le truststore SAML du nœud de passerelle à l'aide duquel la signature de réponse SAML sera validée.
-SamlAssertionEncrypted -sae	Requis si vous activez la réponse signée. Défini sur True pour activer l'assertion chiffrée. La valeur par défaut est False.
-EncryptedAssertionPrivateKeyAlias -espa	Requis si vous activez l'assertion chiffrée. Nom d'alias de la clé privée présente dans le keystore SAML du nœud de passerelle à l'aide de laquelle la clé utilisée pour chiffrer l'assertion sera déchiffrée.
-EncryptedAssertionPrivateKeyPassword -espp	Requis si vous activez l'assertion chiffrée. Mot de passe permettant d'accéder à la clé privée utilisée pour le déchiffrement de la clé de chiffrement de l'assertion
-EnablePasswordComplexity -pc	Facultatif. Activez la complexité du mot de passe pour valider le niveau de sécurité correspondant. Pour un compte utilisateur natif, si vous activez la complexité du mot de passe, utilisez les directives suivantes lorsque vous créez ou modifiez un mot de passe : <ul style="list-style-type: none"> - Le mot de passe doit contenir au moins huit caractères. - Il doit être composé d'un caractère alphabétique, d'un caractère numérique et d'un caractère non alphanumérique, tels que : ! \ " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { } ~ Lorsque vous utilisez des caractères spéciaux dans un mot de passe, il arrive que l'interpréteur de commandes les lise différemment. Par exemple, \$ est interprété comme une variable. Dans ce cas, utilisez un caractère d'échappement pour échapper le caractère spécial.
-AdminconsolePort -ap	Port d'accès à Informatica Administrator.
-HttpsPort -hs	Facultatif. Numéro de port pour sécuriser la connexion à l'outil Administrator tool. Définissez ce numéro de port si vous souhaitez configurer HTTPS pour un nœud.
-KeystoreFile -kf	Facultatif. Le fichier keystore contenant les clés et les certificats est requis si vous utilisez le protocole de sécurité SSL.
-KeystorePass -kp	Facultatif. Mot de passe en texte brut du fichier keystore. Vous pouvez définir un mot de passe avec l'option -kp ou la variable d'environnement INFA_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -kp est prioritaire.
-MinProcessPort -mi	Requis. Numéro de port minimal pour les processus de service d'application exécutés sur le nœud.
-MaxProcessPort -ma	Requis. Numéro de port maximal pour les processus de service d'application exécutés sur le nœud.

Option	Description
-ServerPort -sv	Facultatif. Numéro de port TCP/IP utilisé par le gestionnaire de service. Ce port permet au gestionnaire de service d'écouter les commandes d'arrêt en provenance des composants du domaine. Définissez ce numéro de port si vous avez plusieurs nœuds sur une machine ou si le numéro de port par défaut est utilisé. La valeur par défaut est le numéro de port du nœud plus un.
-AdminconsoleShutdownPort -asp	Numéro de port qui contrôle l'arrêt d'Informatica Administrator.
-BackupDirectory -bd	Facultatif. Répertoire de stockage des fichiers de sauvegarde du référentiel. Le nœud doit avoir accès au répertoire.
-ServiceResilienceTimeout -sr	Facultatif. Temps en secondes disponible pour qu' <i>infasetup</i> essaye d'établir ou de rétablir une connexion au domaine local. Si vous omettez cette option, <i>infasetup</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous ne voyez pas une valeur spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.
-ErrorLogLevel -el	Facultatif. Niveau de gravité des événements de journal dans le journal de domaine. La valeur par défaut est Informations.
-ResourceFile -rf	Requis. Fichier contenant la liste des ressources disponibles pour le nœud. Utilisez le fichier nodeoptions.xml situé à l'emplacement suivant : <code><Informatica installation directory>/isp/bin</code>
-TimeZone -tz	Facultatif. Fuseau horaire utilisé par le gestionnaire de journaux lorsqu'il génère les fichiers d'événements du journal. La valeur par défaut est GMT +00:00. Configurez le fuseau horaire dans le format suivant : GMT (+/-) hh:mm
-Force -f	Facultatif. Écrase la base de données si une base de données avec le même nom existe déjà. N'inclure aucun caractère après cette option.
-TrustedConnection -tc	Facultatif. Connexion à la base de données Microsoft SQL Server via une connexion approuvée. L'authentification de confiance utilise les justificatifs d'identité de sécurité Windows de l'utilisateur en cours pour effectuer la connexion à Microsoft SQL Server. Remarque: Si vous utilisez une connexion approuvée, configurez l'option DatabaseConnectionString.
-DatabaseTruststoreLocation -dbtl	Chemin et nom du fichier truststore de la base de données du référentiel de domaine sécurisé. Obligatoire si vous configurez une base de données du référentiel de domaine sécurisé pour le domaine.
EnableHsts -hsts	Facultatif. Défini sur TRUE pour activer la sécurité de transport HTTP stricte. La sécurité de transport HTTP stricte nécessite que les applications Web utilisent le protocole HTTPS.
* Remarque : si vous exécutez actuellement des scripts qui utilisent cette commande pour activer un keystore personnalisé pour l'authentification SAML, vous devez les mettre à jour afin d'y inclure cette option.	

Si vous exécutez DefineDomain sur un nœud hébergeant actuellement un domaine, reconfigurez les propriétés de domaine suivantes :

- **Services d'application.** Recréer un service d'application qui a été exécuté sur le domaine.
- **Utilisateurs.** Recréer des utilisateurs.
- **Nœuds de passerelle** Configurer les nœuds de passerelle du domaine.
- **Propriétés générales du domaine.** Configurer le délai de résilience et le nombre maximal de tentatives de redémarrage pour le domaine.
- **Grilles.** Recréer une grille quelconque dans le domaine.
- **Authentification LDAP.** Configurer l'authentification LDAP du domaine.
- **Propriétés du gestionnaire de journalisation.** Configurer le chemin d'accès du répertoire partagé du Gestionnaire de journalisation, purger les propriétés et le fuseau horaire.

Si vous modifiez le nom d'hôte ou le numéro de port du nœud de passerelle, vous devez aussi ajouter chaque nœud au domaine à l'aide de la commande *infacmd* AddDomainNode.

DefineGatewayNode

Définit un nœud de passerelle sur la machine actuelle. Cette commande écrase le fichier nodemeta.xml stockant les métadonnées de configuration pour le nœud. Après avoir défini le nœud, exécutez la commande *infacmd* isp AddDomainNode pour l'ajouter au domaine.

La syntaxe de la commande DefineGatewayNode est la suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'*infasetup* DefineGatewayNode :

Option	Description
-DatabaseAddress -da	Obligatoire si vous n'utilisez pas l'option -DatabaseConnectionString (-cs). Nom et numéro du port de la machine hébergeant la base de données de configuration du domaine.
-DatabaseConnectionString -cs	Obligatoire si vous n'utilisez pas les options -DatabaseAddress (-da) et --DatabaseServiceName (-ds). Chaîne de connexion utilisée pour se connecter à la base de données de configuration du domaine. La chaîne de connexion doit inclure l'hôte de la base de données, le port de la base de données et le nom du service de base de données. Placez la chaîne de connexion entre guillemets.
-DatabaseUserName -du	Obligatoire si vous n'utilisez pas l'option -TrustedConnection (-tc). Compte de la base de données qui contient les informations de configuration du domaine.
-DatabasePassword -dp	Mot de passe de la base de données de configuration du domaine correspondant à l'utilisateur de la base de données. Si vous omettez cette option, <i>infasetup</i> utilisera le mot de passe spécifié dans la variable d'environnement INFA_DEFAULT_DATABASE_PASSWORD. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, vous devez entrer un mot de passe à l'aide de cette option.
-DatabaseType -dt	Requis. Type de base de données contenant les métadonnées de configuration du domaine. Les types de base de données sont les suivants : <ul style="list-style-type: none"> - db2 - oracle - mssqlserver - sybase - postgresql
-DatabaseServiceName -ds	Obligatoire si vous n'utilisez pas l'option -DatabaseConnectionString (-cs). Nom du service de base de données. Obligatoire pour les bases de données Oracle, IBM DB2 et Microsoft SQL Server. Entrez le SID pour Oracle, le nom du service pour IBM DB2 ou le nom de la base de données pour Microsoft SQL Server.
-DomainName -dn	Requis. Nom du domaine.

Option	Description
-nodeName -nn	Facultatif. Nom du nœud. Les noms de nœud doivent avoir une longueur comprise entre 1 et 79 caractères et ne peuvent contenir ni des espaces, ni les caractères suivants : \ / * ? < > "
-NodeAddress -na	Facultatif. Nom d'hôte et numéro de port de la machine hébergeant le nœud. Choisissez un numéro de port disponible.
-ServiceManagerPort -sp	Facultatif. Numéro de port utilisé par le gestionnaire de service pour écouter les demandes de connexions entrantes.
-EnableTLS -tls	Facultatif. Configure la communication sécurisée des services dans le domaine Informatica. Si vous utilisez les certificats SSL par défaut fournis par Informatica, vous n'avez pas besoin de spécifier les options keystore et truststore. Si vous n'utilisez pas le certificat SSL par défaut, vous devez spécifier les options keystore et truststore. Les valeurs valides sont True ou False. La valeur par défaut est false. Si vous spécifiez l'option -tls sans valeur, le domaine Informatica utilise la communication sécurisée entre les services. Pour activer la communication sécurisée pour les services ou applications Web associés, tels que l'outil Administrator tool, l'outil Analyst tool ou le hub de services Web, configurez la communication sécurisée séparément dans les applications.
-NodeKeystore -nk	Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Obligatoire si vous utilisez vos certificats SSL. Répertoire contenant les fichiers keystore. Le domaine Informatica requiert les certificats SSL au format PEM et dans des fichiers Java Keystore (JKS). Le répertoire doit contenir les fichiers keystore aux formats PEM et JKS. Les fichiers keystore doivent être nommés infa_keystore.jks et infa_keystore.pem. Si le fichier keystore que vous recevez de l'autorité de certification (CA) a un nom différent, vous devez le renommer infa_keystore.jks et infa_keystore.pem. Vous devez utiliser le même fichier keystore pour tous les nœuds du domaine.
-NodeKeystorePass -nkp	Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Obligatoire si vous utilisez vos certificats SSL. Mot de passe pour le fichier keystore infa_keystore.jks.
-NodeTruststore -nt	Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Obligatoire si vous utilisez vos certificats SSL. Répertoire contenant les fichiers truststore. Le domaine Informatica requiert les certificats SSL au format PEM et dans des fichiers Java Keystore (JKS). Le répertoire doit contenir les fichiers truststore aux formats PEM et JKS. Les fichiers truststore doivent être nommés infa_truststore.jks et infa_truststore.pem. Si le fichier truststore que vous recevez de l'autorité de certification (CA) a un nom différent, vous devez le renommer infa_truststore.jks et infa_truststore.pem.
-NodeTruststorePass -ntp	Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Obligatoire si vous utilisez vos certificats SSL. Mot de passe du fichier infa_truststore.jks.

Option	Description
-CipherWhiteList -cwl	Facultatif. Liste séparée par des virgules de suites de chiffrement JSSE que vous souhaitez ajouter à la liste effective. Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.
-CipherBlackList -cbl	Facultatif. Liste séparée par des virgules de suites de chiffrement JSSE que vous souhaitez supprimer de la liste effective. Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.
-CipherWhiteListFile -cwlf	Facultatif. Nom de fichier absolu du fichier en texte brut qui contient une liste de suites de chiffrement séparée par des virgules à ajouter à la liste effective. Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.
-CipherBlackListFile -cblf	Facultatif. Nom de fichier absolu du fichier en texte brut qui contient une liste de suites de chiffrement séparée par des virgules que vous souhaitez supprimer de la liste effective. Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.
-EnableKerberos -krb	Facultatif. Configure le domaine Informatica pour qu'il utilise l'authentification Kerberos. Les valeurs valides sont True ou False. Si la valeur est True, le domaine utilise l'authentification Kerberos et vous ne pouvez plus changer le mode d'authentification. Après avoir activé l'authentification Kerberos, vous ne pouvez pas la désactiver. La valeur par défaut est False. Si vous spécifiez l'option -krb sans valeur, le domaine Informatica utilise l'authentification Kerberos.
-ServiceRealmName -srn	Facultatif. Nom du domaine Kerberos utilisé pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules. Pour configurer l'authentification Kerberos inter-domaines, spécifiez le nom de chaque domaine Kerberos utilisé pour l'authentification des utilisateurs, séparé par une virgule. Par exemple : COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple, spécifiez la valeur suivante afin d'inclure tous les domaines qui incluent le nom EAST.COMPANY.COM : *EAST.COMPANY.COM
-UserRealmName -urn	Facultatif. Nom du domaine Kerberos utilisé pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules. Pour configurer l'authentification Kerberos inter-domaines, spécifiez le nom de chaque domaine Kerberos utilisé pour l'authentification des utilisateurs, séparé par une virgule. Par exemple : COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple, spécifiez la valeur suivante afin d'inclure tous les domaines qui incluent le nom EAST.COMPANY.COM : *EAST.COMPANY.COM

Option	Description
-KeysDirectory -kd	Facultatif. Répertoire dans lequel sont stockés tous les fichiers Keytab et la clé de cryptage pour le domaine Informatica. La valeur par défaut est <InformaticaInstallationDir>/isp/config/keys.
-EnableSaml -saml	Facultatif. Active ou désactive l'authentification SAML dans le domaine Informatica. Définissez cette valeur sur True pour activer l'authentification SAML dans le domaine Informatica. La valeur par défaut est False.
-SamlTrustStoreDir -std	Facultatif. Répertoire contenant le fichier truststore personnalisé requis pour utiliser l'authentification SAML sur le nœud de passerelle. Spécifiez le répertoire uniquement, pas le chemin d'accès complet au fichier. La valeur par défaut du fichier truststore d'Informatica est utilisée si aucun fichier truststore n'est spécifié.
-SamlTrustStorePassword -stp	Obligatoire si vous utilisez un fichier truststore personnalisé pour l'authentification SAML. Mot de passe pour le fichier truststore personnalisé.
-SamlKeyStoreDir -skd	Facultatif. Répertoire contenant le fichier keystore personnalisé requis pour utiliser l'authentification SAML sur le nœud de passerelle. Spécifiez le répertoire uniquement, pas le chemin d'accès complet au fichier.
-SamlKeyStorePassword -skp	Obligatoire si vous utilisez un fichier keystore personnalisé pour l'authentification SAML. Mot de passe du keystore SAML. *
-AdminconsolePort -ap	Facultatif. Port d'accès à Informatica Administrator.
-HttpsPort -hs	Facultatif. Numéro de port utilisé par le nœud pour la communication entre l'outil Administrator tool et le Gestionnaire de service. Définissez ce numéro de port si vous souhaitez configurer HTTPS pour un nœud. Pour désactiver le support HTTPS pour un nœud, initialisez ce numéro à zéro.
-KeystoreFile -kf	Facultatif. Le fichier keystore contenant les clés et les certificats est requis si vous utilisez le protocole de sécurité SSL.
-KeystorePass -kp	Facultatif. Mot de passe en texte brut du fichier keystore. Vous pouvez définir un mot de passe avec l'option -kp ou la variable d'environnement INFA_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -kp est prioritaire.
-MinProcessPort -mi	Facultatif. Numéro de port minimal pour les processus de service d'application exécutés sur le nœud. Par défaut 11000.
-MaxProcessPort -ma	Facultatif. Numéro de port maximal pour les processus de service d'application exécutés sur le nœud. Par défaut 11999.
-LogServiceDirectory -ld	Requis. Chemin du répertoire partagé utilisé par le gestionnaire de journaux pour stocker des fichiers d'événements de journal. Vérifiez que -ld ne correspond pas à la valeur--sld spécifiée ni ne la contient.

Option	Description
-SystemLogDirectory -sld	Facultatif. Chemin du répertoire pour stocker les fichiers journaux système. Vérifiez que -ld ne correspond pas à la valeur--sld spécifiée ni ne la contient. La valeur par défaut est <INFA_home>/logs.
-ServerPort -sv	Facultatif. Numéro de port TCP/IP utilisé par le gestionnaire de service. Le gestionnaire de service utilise ce port pour écouter les commandes d'arrêt des composants PowerCenter. Définissez ce numéro de port si vous avez plusieurs nœuds sur une machine ou si le numéro de port par défaut est utilisé. La valeur par défaut est 8 005.
-AdminconsoleShutdownPort -asp	Facultatif. Numéro de port qui contrôle l'arrêt d'Informatica Administrator.
-BackupDirectory -bd	Facultatif. Répertoire de stockage des fichiers de sauvegarde du référentiel. Le nœud doit avoir accès au répertoire.
-ErrorLogLevel -el	Facultatif. Niveau de gravité des événements de journal dans le journal de domaine. La valeur par défaut est Informations.
-ResourceFile -rf	Requis. Fichier contenant la liste des ressources disponibles pour le nœud. Utilisez le fichier nodeoptions.xml qui se trouve à l'emplacement suivant : <INFA_HOME>/isp/bin .
-Tablespace -ts	Obligatoire dans le cas d'une base de données IBM DB2. Nom de l'espace de table dans lequel se situent les tables de la base de données de configuration du domaine.
-SchemaName -sc	Facultatif. Nom du schéma Microsoft SQL Server. Entrez un nom de schéma si vous n'utilisez pas le schéma par défaut.
-DatabaseTlsEnabled -dbtls	Facultatif. Indique si la base de données du domaine Informatica est sécurisée avec le protocole TLS ou SSL. Définissez cette option sur True pour la base de données sécurisée. La valeur par défaut est false. Si vous spécifiez l'option -dbtls sans valeur, le domaine Informatica utilise la communication sécurisée à la base de données du domaine Informatica.
-DatabaseTruststorePassword -dbtp	Facultatif. Mot de passe du fichier truststore de la base de données sécurisée.
-TrustedConnection -tc	Facultatif. Connexion à la base de données Microsoft SQL Server via une connexion approuvée. L'authentification de confiance utilise les justificatifs d'identité de sécurité Windows de l'utilisateur en cours pour effectuer la connexion à Microsoft SQL Server.
-DatabaseTruststoreLocation -dbtl	Chemin et nom du fichier truststore de la base de données du référentiel de domaine sécurisé. Obligatoire si vous configurez une base de données du référentiel de domaine sécurisé pour le domaine.
* Remarque : si vous exécutez actuellement des scripts qui utilisent cette commande pour activer un keystore personnalisé pour l'authentification SAML, vous devez les mettre à jour afin d'y inclure cette option.	

LIENS CONNEXES :

- [“AddDomainNode” à la page 361](#)

DefineWorkerNode

Définit un nœud de travail sur la machine actuelle. infasetup crée le fichier nodemeta.xml stockant les métadonnées de configuration du nœud. Si vous exécutez cette commande sur un nœud existant, les métadonnées de configuration de ce nœud seront écrasées. Après avoir défini le nœud, exécutez la commande infacmd isp AddDomainNode pour l'ajouter au domaine.

La commande DefineWorkerNode utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'infasetup DefineWorkerNode :

Option	Description
-DomainName -dn	Requis. Nom du domaine auquel le nœud de travail est relié.
-NodeName -nn	Requis. Nom du nœud. Les noms de nœud doivent avoir une longueur comprise entre 1 et 79 caractères et ne peuvent contenir ni des espaces, ni les caractères suivants : \ / * ? < > "
-NodeAddress -na	Requis. Nom d'hôte et numéro de port de la machine hébergeant le nœud. Choisissez un numéro de port disponible.

Option	Description
-ServiceManagerPort -sp	Facultatif. Numéro de port utilisé par le gestionnaire de service pour écouter les demandes de connexions entrantes.
-EnableTLS -tls	<p>Facultatif. Configure la communication sécurisée des services dans le domaine Informatica.</p> <p>Si vous utilisez les certificats SSL par défaut fournis par Informatica, vous n'avez pas besoin de spécifier les options keystore et truststore. Si vous n'utilisez pas le certificat SSL par défaut, vous devez spécifier les options keystore et truststore. Les valeurs valides sont True ou False. La valeur par défaut est false. Si vous spécifiez l'option -tls sans valeur, le domaine Informatica utilise la communication sécurisée entre les services.</p> <p>Pour activer la communication sécurisée pour les services ou applications Web associés, tels que l'outil Administrator tool, l'outil Analyst tool ou le hub de services Web, configurez la communication sécurisée séparément dans les applications.</p>
-NodeKeystore -nk	<p>Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Requis si vous utilisez vos certificats SSL. Répertoire contenant les fichiers keystore. Le domaine Informatica requiert les certificats SSL au format PEM et dans des fichiers Java Keystore (JKS). Le répertoire doit contenir les fichiers keystore aux formats PEM et JKS.</p> <p>Les fichiers keystore doivent être nommés infa_keystore.jks et infa_keystore.pem. Si le fichier keystore que vous recevez de l'autorité de certification (CA) a un nom différent, vous devez le renommer infa_keystore.jks et infa_keystore.pem.</p> <p>Vous devez utiliser le même fichier keystore pour tous les nœuds du domaine.</p>
-NodeKeystorePass -nkp	Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Requis si vous utilisez vos certificats SSL. Mot de passe pour le fichier keystore infa_keystore.jks.
-NodeTruststore -nt	<p>Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Répertoire contenant les fichiers truststore. Le domaine Informatica requiert les certificats SSL au format PEM et dans des fichiers Java Keystore (JKS). Le répertoire doit contenir les fichiers truststore aux formats PEM et JKS.</p> <p>Les fichiers truststore doivent être nommés infa_truststore.jks et infa_truststore.pem. Si le fichier truststore que vous recevez de l'autorité de certification (CA) a un nom différent, vous devez le renommer infa_truststore.jks et infa_truststore.pem.</p>
-NodeTruststorePass -ntp	Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Requis si vous utilisez vos certificats SSL. Mot de passe du fichier infa_truststore.jks.
-CipherWhiteList -cwl	<p>Facultatif. Liste séparée par des virgules de suites de chiffrement JSSE que vous souhaitez ajouter à la liste effective.</p> <p>Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.</p>
-CipherBlackList -cbl	<p>Facultatif. Liste séparée par des virgules de suites de chiffrement JSSE que vous souhaitez supprimer de la liste effective.</p> <p>Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.</p>
-CipherWhiteListFile -cwlf	<p>Facultatif. Nom de fichier absolu du fichier en texte brut qui contient une liste de suites de chiffrement séparée par des virgules à ajouter à la liste effective.</p> <p>Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.</p>
-CipherBlackListFile -cbIf	<p>Facultatif. Nom de fichier absolu du fichier en texte brut qui contient une liste de suites de chiffrement séparée par des virgules que vous souhaitez supprimer de la liste effective.</p> <p>Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.</p>

Option	Description
-EnableKerberos -krb	Facultatif. Configure le domaine Informatica pour qu'il utilise l'authentification Kerberos. Les valeurs valides sont True ou False. Si la valeur est True, le domaine utilise l'authentification Kerberos et vous ne pouvez plus changer le mode d'authentification. Après avoir activé l'authentification Kerberos, vous ne pouvez pas la désactiver. La valeur par défaut est False. Si vous spécifiez l'option -krb sans valeur, le domaine Informatica utilise l'authentification Kerberos.
-ServiceRealmName -srn	Facultatif. Nom du domaine Kerberos utilisé pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules. Pour configurer l'authentification Kerberos inter-domaines, spécifiez le nom de chaque domaine Kerberos utilisé pour l'authentification des utilisateurs, séparé par une virgule. Par exemple : COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple, spécifiez la valeur suivante afin d'inclure tous les domaines qui incluent le nom EAST.COMPANY.COM : *EAST.COMPANY.COM
-UserRealmName -urn	Facultatif. Nom du domaine Kerberos utilisé pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules. Pour configurer l'authentification Kerberos inter-domaines, spécifiez le nom de chaque domaine Kerberos utilisé pour l'authentification des utilisateurs, séparé par une virgule. Par exemple : COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple, spécifiez la valeur suivante afin d'inclure tous les domaines qui incluent le nom EAST.COMPANY.COM : *EAST.COMPANY.COM
-KeysDirectory -kd	Facultatif. Répertoire dans lequel sont stockés tous les fichiers Keytab et la clé de cryptage pour le domaine Informatica. La valeur par défaut est <InformaticaInstallationDir>/isp/config/keys.
-HttpsPort -hs	Facultatif. Numéro de port utilisé par le nœud pour la communication entre l'outil Administrator tool et le Gestionnaire de service. Définissez ce numéro de port si vous souhaitez configurer HTTPS pour un nœud. Pour désactiver le support HTTPS pour un nœud, initialisez ce numéro à zéro.
-NodeKeystoreFile -kf	Facultatif. Le fichier keystore contenant les clés et les certificats est requis si vous utilisez le protocole de sécurité SSL.
-KeystorePass -kp	Facultatif. Mot de passe en texte brut du fichier keystore. Vous pouvez définir un mot de passe avec l'option -kp ou la variable d'environnement INFA_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -kp est prioritaire.
-GatewayAddress -dg	Requis. Nom de machine et numéro de port de l'hôte de passerelle.

Option	Description
-UserName -un	<p>Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire.</p> <p>Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.</p>
-SecurityDomain -sdn	<p>Nom du domaine de sécurité que vous voulez créer et auquel l'utilisateur du domaine appartient. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Vous pouvez spécifier une valeur pour -sdn ou utiliser la valeur par défaut selon le mode d'authentification :</p> <ul style="list-style-type: none"> - Obligatoire si le domaine utilise l'authentification LDAP. La valeur par défaut est Native. Pour travailler avec l'authentification LDAP, vous devez spécifier la valeur pour -sdn. - Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. La valeur par défaut est natif pour l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Password -pd	<p>Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p>
-MinProcessPort -mi	<p>Facultatif. Numéro de port minimal pour les processus de service d'application exécutés sur le nœud. Par défaut 11000.</p>
-MaxProcessPort -ma	<p>Facultatif. Numéro de port maximal pour les processus de service d'application exécutés sur le nœud. Par défaut 11999.</p>
-ServerPort -sv	<p>Facultatif. Numéro de port TCP/IP utilisé par le gestionnaire de service. Le gestionnaire de service utilise ce port pour écouter les commandes d'arrêt des composants PowerCenter. Définissez ce numéro de port si vous avez plusieurs nœuds sur une machine ou si le numéro de port par défaut est utilisé. La valeur par défaut est 8 005.</p>
-BackupDirectory -bd	<p>Facultatif. Répertoire de stockage des fichiers de sauvegarde du référentiel. Le nœud doit avoir accès au répertoire.</p>
-ErrorLogLevel -el	<p>Facultatif. Niveau de gravité des événements de journal dans le journal de domaine. Un des suivants :</p> <ul style="list-style-type: none"> - irrécupérable - erreur - avertissement - informations - trace - déboguer <p>La valeur par défaut est Informations.</p>

Option	Description
-ResourceFile -rf	Requis. Fichier contenant la liste des ressources disponibles pour le nœud. Utilisez le fichier nodeoptions.xml qui se trouve à l'emplacement suivant : <INFA_HOME>/isp/bin .
-SystemLogDirectory -sld	Facultatif. Chemin du répertoire pour stocker les fichiers journaux système. La valeur par défaut est <INFA_home>/logs.
-EnableSaml -saml	Facultatif. Active ou désactive l'authentification SAML dans le domaine Informatica. Définissez cette valeur sur True pour activer l'authentification SAML dans le domaine Informatica. La valeur par défaut est False.
-SamlTrustStoreDir -std	Facultatif. Répertoire contenant le fichier truststore personnalisé requis pour utiliser l'authentification SAML sur le nœud de passerelle. Spécifiez le répertoire uniquement, pas le chemin d'accès complet au fichier. La valeur par défaut du fichier truststore d'Informatica est utilisée si aucun fichier truststore n'est spécifié.
-SamlTrustStorePassword -stp	Requis si vous utilisez un fichier truststore personnalisé pour l'authentification SAML. Mot de passe pour le fichier truststore personnalisé.
-SamlKeyStoreDir -skd	Facultatif. Répertoire contenant le fichier keystore personnalisé requis pour utiliser l'authentification SAML sur le nœud de passerelle. Spécifiez le répertoire uniquement, pas le chemin d'accès complet au fichier.
-SamlKeyStorePassword -skp	Obligatoire si vous utilisez un fichier keystore personnalisé pour l'authentification SAML. Mot de passe du keystore SAML. *
* Remarque : si vous exécutez actuellement des scripts qui utilisent cette commande pour activer un keystore personnalisé pour l'authentification SAML, vous devez les mettre à jour afin d'y inclure cette option.	

DeleteDomain

Supprime les tables des métadonnées du domaine. Avant d'exécuter cette commande, vous devez arrêter les services Informatica sur la machine. Pour supprimer un domaine dans un environnement Windows, vous devez aussi ouvrir le port hôte ou désactiver le pare-feu.

Si la commande échoue en indiquant une erreur de mémoire Java, augmentez la mémoire système allouée à la commande infasetup. Pour augmenter la mémoire système, définissez la valeur -Xmx dans la variable d'environnement INFA_JAVA_CMD_OPTS.

La commande DeleteDomain utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'*infasetup* DeleteDomain :

Option	Argument	Description
-DatabaseAddress -da	database_hostname:database_port	Requis si vous n'utilisez pas l'option - DatabaseConnectionString (-cs). Nom et numéro du port de la machine hébergeant la base de données de configuration du domaine.
-DatabaseConnectionString -cs	database_connection_string	Requis si vous n'utilisez pas les options - DatabaseAddress (-da) et - DatabaseServiceName (-ds). Chaîne de connexion utilisée pour se connecter à la base de données de configuration du domaine. La chaîne de connexion doit inclure l'hôte de la base de données, le port de la base de données et le nom du service de base de données. Placez la chaîne de connexion entre guillemets.
-DatabaseUserName -du	database_user_name	Requis si vous n'utilisez pas l'option - TrustedConnection (-tc). Compte de la base de données qui contient les informations de configuration du domaine.
-DatabasePassword -dp	database_password	Mot de passe de la base de données de configuration du domaine correspondant à l'utilisateur de la base de données. Si vous omettez cette option, <i>infasetup</i> utilisera le mot de passe spécifié dans la variable d'environnement INFA_DEFAULT_DATABASE_PASSWORD. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, vous devez entrer un mot de passe à l'aide de cette option.
-DatabaseType -dt	database_type	Requis. Type de base de données contenant les métadonnées de configuration du domaine. Les types de base de données sont les suivants : <ul style="list-style-type: none"> - db2 - oracle - mssqlserver - sybase - postgresql

Option	Argument	Description
-DatabaseServiceName -ds	database_service_name	Requis si vous n'utilisez pas l'option - DatabaseConnectionString (-cs). Nom du service de base de données. Requis pour les bases de données Oracle, IBM DB2 et Microsoft SQL Server. Entrez le SID pour Oracle, le nom du service pour IBM DB2 ou le nom de la base de données pour Microsoft SQL Server.
-Tablespace -ts	tablespace_name	Requis dans le cas d'une base de données IBM DB2. Nom de l'espace de table dans lequel se situent les tables de la base de données de configuration du domaine.
SchemaName -sc	schema_name	Facultatif. Nom du schéma Microsoft SQL Server ou PostgreSQL. Entrez un nom de schéma si vous n'utilisez pas le schéma par défaut.
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Facultatif. Indique si la base de données du domaine Informatica est sécurisée avec le protocole TLS ou SSL. Définissez cette option sur True pour la base de données sécurisée. La valeur par défaut est false. Si vous spécifiez l'option -dbtls sans valeur, le domaine Informatica utilise la communication sécurisée avec la base de données du domaine Informatica.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Facultatif. Mot de passe du fichier truststore de la base de données sécurisée.
-TrustedConnection -tc	-	Facultatif. Connexion à la base de données Microsoft SQL Server via une connexion approuvée. L'authentification de confiance utilise les justificatifs d'identité de sécurité Windows de l'utilisateur en cours pour effectuer la connexion à Microsoft SQL Server.
-EncryptionKeyLocation -kl	encryption_key_location	Répertoire contenant la clé de cryptage actuelle. Le nom du fichier de chiffrement est sitekey. Informatica change le nom du fichier sitekey actuel en sitekey_old et génère une clé de chiffrement dans un nouveau fichier nommé sitekey dans le même répertoire.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Chemin et nom du fichier truststore de la base de données du référentiel de domaine sécurisé. Requis si vous configurez une base de données du référentiel de domaine sécurisé pour le domaine.

GenerateEncryptionKey

Générez une clé de cryptage pour sécuriser les données sensibles, telles que les mots de passe, dans le domaine Informatica.

La syntaxe de la commande GenerateEncryptionKey est la suivante :

```
GenerateEncryptionKey [<-EncryptionKeyLocation|-kl> encryption_key_location]
```

-EncryptionKeyLocation. Répertoire contenant la clé de chiffrement actuelle. Le nom du fichier de chiffrement est *sitekey*. Informatica remplace le nom du fichier *sitekey* actuel par *sitekey_old* et génère une clé de chiffrement dans un nouveau fichier nommé *sitekey* dans le même répertoire.

Pour exécuter à nouveau la commande lorsqu'au moins deux fichiers *sitekey* se trouvent dans le répertoire, assurez-vous de sauvegarder les fichiers *sitekey*. Vous pouvez ensuite exécuter la commande pour créer le fichier *sitekey* avant de restaurer la sauvegarde des fichiers *sitekey*.

Le fichier *sitekey* est unique. Assurez-vous d'enregistrer une copie de cette clé de site unique. En cas de perte, vous ne pouvez plus la régénérer. Ne partagez la clé de site unique avec personne.

Aide

La commande Help affiche les options et arguments d'une commande. Si vous omettez le nom de commande, *infasetup* liste toutes les commandes.

La commande Help utilise la syntaxe suivante :

```
Help [command]
```

Par exemple, si vous saisissez `infasetup Help UpdateWorkerNode`, *infasetup* renvoie les options et les arguments suivants de la commande `UpdateWorkerNode` :

```
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]
```

Le tableau suivant décrit les options et arguments d'*infasetup Help* :

Option	Argument	Description
-	commande	Facultatif. Nom de commande. Si vous omettez le nom de commande, <i>infasetup</i> liste toutes les commandes.

ListDomainCiphers

Afficher une ou plusieurs des listes de suites de chiffres suivantes : liste noire, liste par défaut, liste effective ou liste blanche.

Liste noire

Liste de suites de chiffres que vous souhaitez voir bloquées par le domaine Informatica. Lorsque vous ajoutez une suite de chiffres à la liste noire, le domaine Informatica la supprime de la liste effective. Vous pouvez ajouter à la liste noire des suites de chiffres se trouvant dans la liste par défaut.

Liste par défaut

Liste de suites de chiffres prises en charge par défaut par le domaine Informatica.

Liste blanche

Liste de suites de chiffres que vous voulez voir prises en charge par le domaine Informatica en plus de la liste par défaut. Lorsque vous ajoutez une suite de chiffres à la liste blanche, le domaine Informatica l'ajoute à la liste effective. Il n'est pas nécessaire d'ajouter les suites de chiffres de la liste par défaut à la liste blanche.

La commande ListDomainCiphers utilise la syntaxe suivante :

```
[<-list|-l>] ALL|BLACK|DEFAULT|EFFECTIVE|WHITE  
[<-domainConfig|-dc> true|false]
```

Remarque: Vous ne pouvez pas exécuter cette commande sur un nœud de travail.

Le tableau suivant décrit les options et arguments d'infasetup listDomainCiphers :

Option	Argument	Description
-list -l	ALL BLACK DEFAULT EFFECTIVE WHITE	Facultatif. Liste de configurations de suites de chiffres à afficher. L'argument ALL affiche la liste noire, la liste par défaut, la liste effective et la liste blanche. L'argument BLACK affiche la liste noire. L'argument DEFAULT affiche la liste par défaut. L'argument EFFECTIVE affiche la liste effective. L'argument WHITE affiche la liste blanche. Remarque: Les arguments sont sensibles à la casse. Lorsque vous exécutez la commande sur un nœud de passerelle et omettez cette option, la commande affiche toutes les listes de configurations de suites de chiffres.
-domainConfig -dc	True False	Facultatif. Affichez les listes de suites de chiffres du domaine Informatica ou du nœud de passerelle sur lequel vous exécutez la commande. Par défaut, la commande affiche les listes de suites de chiffres du domaine. Définissez cette option sur True pour afficher les listes de suites de chiffres du domaine. Définissez cette option sur False pour afficher les listes de suites de chiffres du nœud de passerelle sur lequel vous exécutez la commande. Remarque: Vous ne pouvez pas afficher les listes blanches ou les listes noires sur des nœuds de passerelle.

MigrateEncryptionKey

Modifier la clé de cryptage utilisée pour sécuriser les données sensibles, telles que les mots de passe, dans le domaine Informatica.

```
MigrateEncryptionKey  
  
<-LocationOfEncryptionKeys|-loc> location_of_encryption_keys  
  
[<-IsDomainMigrated|-mig> is_domain_migrated]
```

Le tableau suivant décrit les options et arguments d'*infasetup* MigrateEncryptionKey :

Option	Argument	Description
-LocationOfEncryptionKeys -loc	location_of_encryption_keys	Requis. Répertoire dans lequel l'ancien fichier de clé de cryptage (siteKey_old) et le nouveau (siteKey) sont stockés. Le répertoire doit contenir les deux fichiers de clé de cryptage, l'ancien et le nouveau. S'ils sont stockés dans des répertoires différents, copiez-les dans le même répertoire. Si le domaine comporte plusieurs nœuds, ce répertoire doit être accessible au nœud du domaine depuis lequel vous exécutez la commande migrateEncryptionKey.
-IsDomainMigrated -mig	is_domain_migrated	Facultatif. Indique si le domaine a été mis à jour de manière à utiliser la clé de cryptage la plus récente. Lorsque vous exécutez la commande migrateEncryptionKey pour la première fois, définissez cette option sur False pour indiquer que le domaine utilise l'ancienne clé de cryptage. Par la suite, lorsque vous exécutez la commande migrateEncryptionKey pour mettre à jour d'autres nœuds du domaine, définissez cette option sur True pour indiquer que le domaine a été mis à jour et utilise la clé de cryptage la plus récente. Vous pouvez également exécuter la commande migrateEncryptionKey sans cette option. La valeur par défaut est True.

RestoreDomain

Restaure les métadonnées de configuration pour le domaine à partir d'un fichier de sauvegarde .mrep. Si vous avez un fichier de sauvegarde d'une précédente version d'Informatica, vous devez utiliser l'ancienne version pour restaurer le domaine.

Vous devez arrêter le domaine avant d'exécuter cette commande.

Si vous restaurez le domaine dans une base de données autre que la base de données de sauvegarde d'origine, vous devez restaurer le contenu de la table ISP_RUN_LOG pour obtenir le flux de travail et les journaux de session précédents.

Si la commande échoue en indiquant une erreur de mémoire Java, augmentez la mémoire système allouée à la commande infasetup. Pour augmenter la mémoire système, définissez la valeur -Xmx dans la variable d'environnement INFA_JAVA_CMD_OPTS.

La commande RestoreDomain utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'*infasetup* RestoreDomain :

Option	Argument	Description
-DatabaseAddress -da	database_hostname:database_port	Requis si vous n'utilisez pas l'option -DatabaseConnectionString (-cs). Nom et numéro du port de la machine hébergeant la base de données de configuration du domaine.
-DatabaseConnectionString -cs	database_connection_string	Requis si vous n'utilisez pas les options -DatabaseAddress (-da) et -DatabaseServiceName (-ds). Chaîne de connexion utilisée pour se connecter à la base de données de configuration du domaine. La chaîne de connexion doit inclure l'hôte de la base de données, le port de la base de données et le nom du service de base de données. Placez la chaîne de connexion entre guillemets.
-DatabaseUserName -du	database_user_name	Requis si vous n'utilisez pas l'option -TrustedConnection (-tc). Compte de la base de données qui contient les informations de configuration du domaine.

Option	Argument	Description
-DatabasePassword -dp	database_password	Mot de passe de la base de données de configuration du domaine correspondant à l'utilisateur de la base de données. Si vous omettez cette option, <i>infasetup</i> utilisera le mot de passe spécifié dans la variable d'environnement INFA_DEFAULT_DATABASE_PASSWORD. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, vous devez entrer un mot de passe à l'aide de cette option.
-DatabaseType -dt	database_type	Requis. Type de base de données contenant les métadonnées de configuration du domaine. Les types de base de données sont les suivants : <ul style="list-style-type: none"> - db2 - oracle - mssqlserver - sybase - postgresql
-DatabaseServiceName -ds	database_service_name	Requis si vous n'utilisez pas l'option - DatabaseConnectionString (-cs). Nom du service de base de données. Requis pour les bases de données Oracle, IBM DB2 et Microsoft SQL Server. Entrez le SID pour Oracle, le nom du service pour IBM DB2 ou le nom de la base de données pour Microsoft SQL Server.
-BackupFile -bf	backup_file_name	Obligatoire. Nom et chemin du fichier de sauvegarde. Si vous ne spécifiez pas de chemin de fichier, <i>infasetup</i> crée le fichier de sauvegarde dans le répertoire actuel.
-Force -f	-	Facultatif. Écrase la base de données si une base de données avec le même nom existe déjà. N'inclure aucun caractère après cette option.
-ClearNodeAssociation -ca	-	Facultatif. Efface les associations de nœuds lors de la restauration du domaine. Par exemple, un domaine sauvegardé contient le nœud « Node1 » sur la machine « MyHost:9090 ». Si vous spécifiez cette option, la connexion entre le nom de nœud « Node1 » et l'adresse « MyHost:9090 » est interrompue lorsque vous restaurez le domaine. Vous pouvez alors associer un autre nœud à « MyHost:9090 ». Si vous ne spécifiez pas cette option, « Node1 » conserve sa connexion à « MyHost:9090 ». Si vous restaurez le domaine et associez un autre nœud à « MyHost:9090 », le nœud ne démarre pas.
-Tablespace -ts	tablespace_name	Requis dans le cas d'une base de données IBM DB2. Nom de l'espace de table dans lequel se situent les tables de la base de données de configuration du domaine.
-SchemaName -sc	schema_name	Facultatif. Nom du schéma Microsoft SQL Server ou PostgreSQL. Entrez un nom de schéma si vous n'utilisez pas le schéma par défaut.

Option	Argument	Description
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Facultatif. Indique si la base de données du domaine Informatica est sécurisée avec le protocole TLS ou SSL. Définissez cette option sur True pour la base de données sécurisée. La valeur par défaut est false. Si vous spécifiez l'option -dbtls sans valeur, le domaine Informatica utilise la communication sécurisée avec la base de données du domaine Informatica.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Facultatif. Mot de passe du fichier truststore de la base de données sécurisée.
-TrustedConnection -tc	-	Facultatif. Connexion à la base de données Microsoft SQL Server via une connexion approuvée. L'authentification de confiance utilise les justificatifs d'identité de sécurité Windows de l'utilisateur en cours pour effectuer la connexion à Microsoft SQL Server.
-EncryptionKeyLocation -kl	encryption_key_location	Facultatif. Répertoire contenant la clé de chiffrement actuelle. Vous devez spécifier l'emplacement de la clé si la clé de chiffrement n'existe pas dans le fichier isp/config/keys/sitekey. Le nom du fichier de chiffrement est sitekey.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Facultatif. Chemin et nom du fichier truststore de la base de données sécurisée. Requis si vous configurez une base de données du référentiel de domaine sécurisé pour le domaine.

restoreMitKerberosLinkage

Restaure les liaisons vers les bibliothèques Kerberos par défaut utilisées par le domaine Informatica pour l'authentification Kerberos. La commande supprime également les liaisons vers les bibliothèques Kerberos personnalisées qui existent au sein du domaine Informatica.

Pour utiliser les bibliothèques Kerberos par défaut dans un domaine Informatica, procédez comme suit :

1. Arrêtez le domaine.
2. Exécutez la commande `infasetup restoreMitKerberosLinkage` sur chaque nœud du domaine.
3. Après avoir exécuté la commande sur tous les nœuds du domaine, démarrez le domaine.

La commande n'utilise aucune option ni aucun argument. Pour exécuter la commande, vous devez disposer des autorisations de lecture et d'écriture sur chaque nœud du domaine Informatica.

SwitchToKerberosMode

Configurer le domaine Informatica pour utiliser l'authentification Kerberos.

La commande SwitchToKerberosMode utilise la syntaxe suivante :

```
SwitchToKerberosMode  
  
<-administratorName|-ad> administrator_name  
  
<-ServiceRealmName|-srn> realm_name_of_node_spn  
  
<-UserRealmName|-urn> realm_name_of_user_spn  
  
[<-SPNShareLevel|-spnSL> SPNShareLevel PROCESS|NODE]
```

Le tableau suivant décrit les options et arguments d'*infasetup* SwitchToKerberosMode :

Option	Argument	Description
-administratorName -ad	administrator_name	<p>Requis. Nom d'utilisateur du compte administrateur du domaine qui est créé lors de la configuration de l'authentification Kerberos. Spécifiez le nom d'un compte qui existe dans Active Directory.</p> <p>Après avoir configuré l'authentification Kerberos, cet utilisateur est inclus dans le domaine de sécurité <i>_infalInternalNamespace</i> que la commande crée.</p> <p>Si un domaine Kerberos unique est utilisé pour authentifier les utilisateurs, spécifiez le nom samAccount.</p> <p>Si le domaine utilise l'authentification Kerberos inter-domaines, spécifiez le nom du principal de l'utilisateur complet, y compris le nom du domaine. Par exemple : sysadmin@COMPANY.COM</p>
-ServiceRealmName -srn	realm_name_of_node_spn	<p>Requis. Nom du domaine Kerberos utilisé pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules.</p> <p>Pour configurer l'authentification Kerberos inter-domaines, spécifiez le nom de chaque domaine Kerberos utilisé pour l'authentification des utilisateurs, séparé par une virgule. Par exemple : COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple, spécifiez la valeur suivante afin d'inclure tous les domaines qui incluent le nom EAST.COMPANY.COM : *EAST.COMPANY.COM</p>

Option	Argument	Description
-UserRealmName -urn	realm_name_of_user_spn	<p>Requis. Nom du domaine Kerberos utilisé pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules.</p> <p>Pour configurer l'authentification Kerberos inter-domaines, spécifiez le nom de chaque domaine Kerberos utilisé pour l'authentification des utilisateurs, séparé par une virgule. Par exemple :</p> <p>COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple, spécifiez la valeur suivante afin d'inclure tous les domaines qui incluent le nom EAST.COMPANY.COM :</p> <p>*EAST.COMPANY.COM</p>
SPNShareLevel -spnSL	SPNShareLevel PROCESS[NODE]	<p>Facultatif. Indique le niveau du principal du service du domaine. Définissez la propriété sur l'un des niveaux suivants :</p> <ul style="list-style-type: none"> - Processus. Le domaine requiert un nom unique de principal du service (SPN) et un fichier Keytab pour chaque nœud et chaque service sur ce nœud. Le nombre de SPN et de fichiers Keytab requis pour chaque nœud dépend du nombre de processus de service exécutés sur le nœud. Recommandé pour les domaines de production. - Nœud. Le domaine utilise un SPN et un fichier Keytab pour le nœud et tous les services exécutés sur celui-ci. Elle requiert également un autre SPN et un autre fichier keytab pour tous les processus HTTP s'exécutant sur le nœud. Recommandé pour les domaines de test et de développement. Recommandé pour les domaines de test et de développement. <p>La valeur par défaut est le processus.</p>

UpdateDomainCiphers

Mettez à jour le domaine Informatica pour utiliser une nouvelle liste effective. Modifiez la liste blanche pour ajouter des suites de chiffres à la liste effective. Modifiez la liste noire pour retirer des suites de chiffres de la liste effective.

Avant d'exécuter la commande, vérifiez que les conditions suivantes sont respectées :

- Le domaine utilise la communication sécurisée dans le domaine ou des connexions sécurisées aux clients Web.
- Le domaine est arrêté.
- Vous pouvez exécuter la commande sur un nœud de passerelle dans le domaine.

La liste effective de suites de chiffres contient les suites de chiffres prises en charge par le domaine Informatica. Lorsque vous exécutez la commande UpdateDomainCiphers, le domaine Informatica crée la liste de suites de chiffres effective en fonction des listes suivantes :

Liste noire

Liste de suites de chiffres que vous souhaitez voir bloquées par le domaine Informatica. Lorsque vous ajoutez une suite de chiffres à la liste noire, le domaine Informatica la supprime de la liste effective. Vous pouvez ajouter à la liste noire des suites de chiffres se trouvant dans la liste par défaut.

Liste par défaut

Liste de suites de chiffres prises en charge par défaut par le domaine Informatica.

Liste blanche

Liste de suites de chiffres que vous voulez voir prises en charge par le domaine Informatica en plus de la liste par défaut. Lorsque vous ajoutez une suite de chiffres à la liste blanche, le domaine Informatica l'ajoute à la liste effective. Il n'est pas nécessaire d'ajouter les suites de chiffres de la liste par défaut à la liste blanche.

Tenez compte des directives suivantes lorsque vous exécutez la commande `UpdateDomainCiphers` :

- Lorsque vous exécutez la commande, vous créez une liste effective qui remplace la version précédente.
- Lorsque vous exécutez la commande et spécifiez une liste blanche ou une liste noire, la nouvelle liste blanche ou liste noire remplace la version précédente.
- La liste effective inclut les suites de chiffres de la liste par défaut et de la liste blanche et exclut celles de la liste noire.
- Lorsque vous exécutez la commande et ne spécifiez pas de liste blanche ou de liste noire, la commande crée une liste effective qui utilise les suites de chiffres de la liste par défaut.
- La liste effective doit contenir au moins une suite de chiffres prise en charge par TLS v1.1 ou 1.2.
- La liste effective doit être une suite de chiffres valide pour Windows, l'environnement d'exécution Java et OpenSSL.

Pour obtenir plus d'informations sur la création des listes blanches et des listes noires pour mettre à jour la liste effective utilisée par le domaine Informatica, consultez le *Guide de sécurité Informatica*.

La commande `UpdateDomainCiphers` utilise la syntaxe suivante :

```
[<-preview|-p> true|false]

[<-cipherWhiteList|-cwl> ciphersuite1,ciphersuite2,...]

[<-cipherWhiteListFile|-cwlf> whitelist_file_name]

[<-cipherBlackList|-cbl> ciphersuite1,ciphersuite2,...]

[<-cipherBlackListFile|-cblf> blacklist_file_name]
```

Le tableau suivant décrit les options et arguments d'infasetup UpdateDomainCiphers :

Option	Argument	Description
-preview -p	True False	Facultatif. Si la valeur est True, la commande affiche la liste effective des suites de chiffres utilisée par le domaine. Si la valeur est False, la commande met à jour les suites de chiffres du domaine Informatica de façon à utiliser la liste effective de suites de chiffres. La valeur par défaut est False.
-cipherWhiteList -cwl	CipherSuiteName01,CiphersuiteName02, ...	Facultatif. Liste de suites de chiffres séparées par des virgules à ajouter à la liste effective. Utilisez le nom complet du registre de suite de chiffres IANA TLS ou une expression Java régulière. Cette liste remplace la liste blanche précédente. Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.
-cipherWhiteListFile -cwlf	whitelist_file_location	Facultatif. Chemin de fichier absolu et nom d'un fichier en texte brut qui contient une liste de suites de chiffres séparée par des virgules à ajouter à la liste effective. Cette liste remplace la liste blanche précédente. Utilisez le nom complet du registre de suite de chiffres IANA TLS ou une expression Java régulière. Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.
-cipherBlackList -cbl	CipherSuiteName01,CiphersuiteName02, ...	Facultatif. Liste de suites de chiffres séparées par des virgules à supprimer de la liste effective. Utilisez le nom complet du registre de suite de chiffres IANA TLS ou une expression Java régulière. Cette liste remplace la liste noire précédente. Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.
-cipherBlackListFile -cblf	blacklist_file_location	Facultatif. Chemin de fichier absolu et nom d'un fichier en texte brut qui contient une liste de suites de chiffres séparées par des virgules à supprimer de la liste effective. Utilisez le nom complet du registre de suite de chiffres IANA TLS ou une expression Java régulière. Cette liste remplace la précédente. Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.

updateDomainName

Modifie le nom de domaine dans la base de données de configuration du domaine.

Pour mettre à jour le nom de domaine, vous devez au préalable sauvegarder le domaine, la clé spécifique au site et les fichiers keytab. Si le référentiel PowerCenter contient un référentiel global, vous devez désinscrire tous les référentiels locaux du référentiel global.

Pour mettre à jour le nom de domaine, exécutez la commande `infasetup updateDomainName` à partir de n'importe quel nœud de passerelle.

Après avoir mis à jour le domaine, effectuez les opérations suivantes :

1. Exécutez les commandes `updateGatewayNode` et `updateWorkerNode` avec le nom de domaine mis à jour pour tous les nœuds de passerelle et de travail.
2. Vous pouvez inscrire le référentiel local avec un référentiel global connecté en utilisant le nom de domaine mis à jour via la commande `pmrep Register`.
3. Vous pouvez créer des fichiers SPN et keytab avec le nom de domaine mis à jour pour l'authentification Kerberos. Copiez les fichiers keytab dans le répertoire `keys`. Vous pouvez continuer à utiliser le fichier de clé de site plus ancien. Si vous devez régénérer la clé de site lorsqu'elle est manquante ou corrompue, vous devez fournir le nom de domaine plus ancien.
4. Vous devez configurer les clients Informatica pour qu'ils utilisent le nom de domaine mis à jour.

La syntaxe de la commande `updateDomainName` est la suivante :

```
updateDomainName
-dn <domain_name>
```

Le tableau suivant décrit les options et arguments d'*infasetup updateDomainName* :

Option	Argument	Description
-DomainName -dn	domain_name	Obligatoire. Modifie le nom de domaine. Les noms de domaine doivent avoir une longueur comprise entre 1 et 79 caractères et ne peuvent contenir ni des espaces, ni les caractères suivants : / * ? < > "

UpdateGatewayNode

Met à jour les informations de connectivité pour un nœud de passerelle sur la machine actuelle. Avant de mettre à jour le nœud de passerelle, exécutez la commande `infacmd isp ShutDownNode` pour arrêter le nœud.

La syntaxe de la commande `UpdateGatewayNode` est la suivante :

```
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|-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]
[<-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]
```

Le tableau suivant décrit les options et arguments d'*infasetup* UpdateGatewayNode :

Option	Description
-DatabaseAddress -da	Obligatoire si vous n'utilisez pas l'option -DatabaseConnectionString (-cs). Nom et numéro du port de la machine hébergeant la base de données de configuration du domaine.
-DatabaseConnectionString -cs	Obligatoire si vous n'utilisez pas les options -DatabaseAddress (-da) et --DatabaseServiceName (-ds). Chaîne de connexion utilisée pour se connecter à la base de données de configuration du domaine. La chaîne de connexion doit inclure l'hôte de la base de données, le port de la base de données et le nom du service de base de données. Placez la chaîne de connexion entre guillemets.
-DatabaseUserName -du	Obligatoire si vous n'utilisez pas l'option -TrustedConnection (-tc). Compte de la base de données qui contient les informations de configuration du domaine.
-DatabasePassword -dp	Mot de passe de la base de données de configuration du domaine correspondant à l'utilisateur de la base de données. Si vous omettez cette option, <i>infasetup</i> utilisera le mot de passe spécifié dans la variable d'environnement INFA_DEFAULT_DATABASE_PASSWORD. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, vous devez entrer un mot de passe à l'aide de cette option.

Option	Description
-DatabaseType -dt	Requis. Type de base de données contenant les métadonnées de configuration du domaine. Les types de base de données sont les suivants : <ul style="list-style-type: none"> - db2 - oracle - mssqlserver - sybase - postgresql
-DatabaseServiceName -ds	Obligatoire si vous n'utilisez pas l'option -DatabaseConnectionString (-cs). Nom du service de base de données. Obligatoire pour les bases de données Oracle, IBM DB2 et Microsoft SQL Server. Entrez le SID pour Oracle, le nom du service pour IBM DB2 ou le nom de la base de données pour Microsoft SQL Server.
-DomainName -dn	Facultatif. Nom du domaine.
-NodeName -nn	Facultatif. Nom du nœud. Les noms de nœud doivent avoir une longueur comprise entre 1 et 79 caractères et ne peuvent contenir ni des espaces, ni les caractères suivants : \ / * ? < > "
-NodeAddress -na	Facultatif. Nom d'hôte et numéro de port de la machine hébergeant le nœud. Choisissez un numéro de port disponible.
-ServiceManagerPort -sp	Facultatif. Numéro de port utilisé par le gestionnaire de service pour écouter les demandes de connexions entrantes.
-EnableTLS -tls	Facultatif. Configure la communication sécurisée des services dans le domaine Informatica. Si vous utilisez les certificats SSL par défaut fournis par Informatica, vous n'avez pas besoin de spécifier les options keystore et truststore. Si vous n'utilisez pas le certificat SSL par défaut, vous devez spécifier les options keystore et truststore. Les valeurs valides sont True ou False. La valeur par défaut est false. Si vous spécifiez l'option -tls sans valeur, le domaine Informatica utilise la communication sécurisée entre les services. Pour activer la communication sécurisée pour les services ou applications Web associés, tels que l'outil Administrator tool, l'outil Analyst tool ou le hub de services Web, configurez la communication sécurisée séparément dans les applications.
-NodeKeystore -nk	Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Obligatoire si vous utilisez vos certificats SSL. Répertoire contenant les fichiers keystore. Le domaine Informatica requiert les certificats SSL au format PEM et dans des fichiers Java Keystore (JKS). Le répertoire doit contenir les fichiers keystore aux formats PEM et JKS. Les fichiers keystore doivent être nommés infa_keystore.jks et infa_keystore.pem. Si le fichier keystore que vous recevez de l'autorité de certification (CA) a un nom différent, vous devez le renommer infa_keystore.jks et infa_keystore.pem. Vous devez utiliser le même fichier keystore pour tous les nœuds du domaine.
-NodeKeystorePass -nkp	Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Obligatoire si vous utilisez vos certificats SSL. Mot de passe pour le fichier keystore infa_keystore.jks.

Option	Description
-NodeTruststore -nt	<p>Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Obligatoire si vous utilisez vos certificats SSL. Répertoire contenant les fichiers truststore. Le domaine Informatica requiert les certificats SSL au format PEM et dans des fichiers Java Keystore (JKS). Le répertoire doit contenir les fichiers truststore aux formats PEM et JKS.</p> <p>Les fichiers truststore doivent être nommés infa_truststore.jks et infa_truststore.pem. Si le fichier truststore que vous recevez de l'autorité de certification (CA) a un nom différent, vous devez le renommer infa_truststore.jks et infa_truststore.pem.</p>
-NodeTruststorePass -ntp	<p>Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Obligatoire si vous utilisez vos certificats SSL. Mot de passe du fichier infa_truststore.jks.</p>
-CipherWhiteList -cwl	<p>Facultatif. Liste séparée par des virgules de suites de chiffrement JSSE que vous souhaitez ajouter à la liste effective.</p> <p>Cette liste remplace la liste blanche précédente.</p> <p>Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.</p>
-CipherBlackList -cbl	<p>Facultatif. Liste séparée par des virgules de suites de chiffrement JSSE que vous souhaitez supprimer de la liste effective.</p> <p>Cette liste remplace la liste noire précédente.</p> <p>Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.</p>
-CipherWhiteListFile -cwlf	<p>Facultatif. Nom de fichier absolu du fichier en texte brut qui contient une liste de suites de chiffrement séparée par des virgules à ajouter à la liste effective.</p> <p>Cette liste remplace la liste blanche précédente.</p> <p>Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.</p>
-CipherBlackListFile -cblf	<p>Facultatif. Nom de fichier absolu du fichier en texte brut qui contient une liste de suites de chiffrement séparée par des virgules que vous souhaitez supprimer de la liste effective.</p> <p>Cette liste remplace la liste noire précédente.</p> <p>Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.</p>
-EnableKerberos -krb	<p>Facultatif. Configure le domaine Informatica pour qu'il utilise l'authentification Kerberos. Les valeurs valides sont True ou False.</p> <p>Si la valeur est True, le domaine utilise l'authentification Kerberos et vous ne pouvez plus changer le mode d'authentification. Après avoir activé l'authentification Kerberos, vous ne pouvez pas la désactiver. La valeur par défaut est False.</p> <p>Si vous spécifiez l'option -krb sans valeur, le domaine Informatica utilise l'authentification Kerberos.</p>

Option	Description
-ServiceRealmName -srn	<p>Facultatif. Nom du domaine Kerberos que le domaine utilise pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules.</p> <p>Pour configurer l'authentification inter-domaines Kerberos, spécifiez le nom de chaque domaine Kerberos que le domaine utilise pour l'authentification des utilisateurs, séparé par une virgule. Par exemple :</p> <p>COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple, spécifiez la valeur suivante afin d'inclure tous les domaines qui incluent le nom EAST.COMPANY.COM :</p> <p>*EAST.COMPANY.COM</p>
-UserRealmName -urn	<p>Facultatif. Nom du domaine Kerberos que le domaine utilise pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules.</p> <p>Pour configurer l'authentification inter-domaines Kerberos, spécifiez le nom de chaque domaine Kerberos que le domaine utilise pour l'authentification des utilisateurs, séparé par une virgule. Par exemple :</p> <p>COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple, spécifiez la valeur suivante afin d'inclure tous les domaines qui incluent le nom EAST.COMPANY.COM :</p> <p>*EAST.COMPANY.COM</p>
-KeysDirectory -kd	<p>Facultatif. Répertoire dans lequel sont stockés tous les fichiers Keytab et la clé de cryptage pour le domaine Informatica. La valeur par défaut est <InformaticaInstallationDir>/isp/config/keys.</p>
-EnableSaml -saml	<p>Facultatif. Active ou désactive l'authentification SAML dans le domaine Informatica.</p> <p>Définissez cette valeur sur True pour activer l'authentification SAML dans le domaine Informatica. La valeur par défaut est False.</p>
-SamlTrustStoreDir -std	<p>Facultatif. Répertoire contenant le fichier truststore personnalisé requis pour utiliser l'authentification SAML sur le nœud de passerelle. Spécifiez le répertoire uniquement, pas le chemin d'accès complet au fichier.</p> <p>La valeur par défaut du fichier truststore d'Informatica est utilisée si aucun fichier truststore n'est spécifié.</p>
-SamlTrustStorePassword -stp	<p>Obligatoire si vous utilisez un fichier truststore personnalisé pour l'authentification SAML. Mot de passe pour le fichier truststore personnalisé.</p>
-SamlKeyStoreDir -skd	<p>Facultatif. Répertoire contenant le fichier keystore personnalisé requis pour utiliser l'authentification SAML sur le nœud de passerelle. Spécifiez le répertoire uniquement, pas le chemin d'accès complet au fichier.</p>
-SamlKeyStorePassword -skp	<p>Obligatoire si vous utilisez un fichier keystore personnalisé pour l'authentification SAML. Mot de passe du keystore SAML. *</p>
-AdminconsolePort -ap	<p>Facultatif. Port d'accès à Informatica Administrator.</p>

Option	Description
-HttpsPort -hs	Facultatif. Numéro de port pour sécuriser la connexion à l'outil Administrator tool. Définissez ce numéro de port si vous souhaitez configurer HTTPS pour un nœud. Pour désactiver le support HTTPS pour un nœud, initialisez ce numéro à zéro.
-KeystoreFile -kf	Facultatif. Le fichier keystore contenant les clés et les certificats est requis si vous utilisez le protocole de sécurité SSL.
-KeystorePass -kp	Facultatif. Mot de passe en texte brut du fichier keystore. Vous pouvez définir un mot de passe avec l'option -kp ou la variable d'environnement INFA_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -kp est prioritaire.
-LogServiceDirectory -ld	Facultatif. Chemin du répertoire partagé utilisé par le gestionnaire de journaux pour stocker des fichiers d'événements de journal. Vérifiez que -ld ne correspond pas à la valeur--sld spécifiée ni ne la contient.
-SystemLogDirectory -sld	Facultatif. Chemin du répertoire pour stocker les fichiers journaux système. Vérifiez que -ld ne correspond pas à la valeur--sld spécifiée ni ne la contient. La valeur par défaut est <INFA_home>/logs.
-ServerPort -sv	Facultatif. Numéro de port TCP/IP utilisé par le gestionnaire de service. Le gestionnaire de service utilise ce port pour écouter les commandes d'arrêt des composants PowerCenter. Définissez ce numéro de port si vous avez plusieurs nœuds sur une machine ou si le numéro de port par défaut est utilisé. La valeur par défaut est 8 005.
-AdminconsoleShutdownPort -asp	Facultatif. Numéro de port qui contrôle l'arrêt d'Informatica Administrator.
-Tablespace -ts	Obligatoire dans le cas d'une base de données IBM DB2. Nom de l'espace de table dans lequel se situent les tables de la base de données de configuration du domaine.
-SchemaName -sc	Facultatif. Nom du schéma Microsoft SQL Server. Entrez un nom de schéma si vous n'utilisez pas le schéma par défaut.
-DatabaseTlsEnabled -dbtls	Facultatif. Indique si la base de données du domaine Informatica est sécurisée avec le protocole TLS ou SSL. Définissez cette option sur True pour la base de données sécurisée. La valeur par défaut est false. Si vous spécifiez l'option -dbtls sans valeur, le domaine Informatica utilise la communication sécurisée avec la base de données du domaine Informatica.
-DatabaseTruststorePassword -dbtp	Facultatif. Mot de passe du fichier truststore de la base de données sécurisée.
-TrustedConnection -tc	Facultatif. Connexion à la base de données Microsoft SQL Server via une connexion approuvée. L'authentification de confiance utilise les justificatifs d'identité de sécurité Windows de l'utilisateur en cours pour effectuer la connexion à Microsoft SQL Server.
-resetHostPort -rst	Obligatoire si vous spécifiez l'option NodeAddress ou ServiceManager. Réinitialise le numéro de port hôte.

Option	Description
-DatabaseTruststoreLocation -dbtl	Facultatif. Chemin et nom du fichier truststore du nœud de passerelle.
* Remarque : si vous exécutez actuellement des scripts qui utilisent cette commande pour activer un keystore personnalisé pour l'authentification SAML, vous devez les mettre à jour afin d'y inclure cette option.	

UpdateKerberosAdminUser

Met à jour l'utilisateur administrateur Kerberos par défaut dans le référentiel du domaine.

La commande UpdateKerberosAdminUser utilise la syntaxe suivante :

```
UpdateKerberosAdminUser
<-KerberosAdminName|-kan> kerberos_admin_name
```

Le tableau suivant décrit les options et les arguments UpdateKerberosAdminUser de la commande *infasetup* :

Option	Argument	Description
-KerberosAdminName -kan	kerberos_admin_name	Requis. Nom de l'utilisateur à sélectionner comme administrateur par défaut. Si un domaine Kerberos unique est utilisé pour authentifier les utilisateurs, spécifiez le nom samAccount. Si le domaine utilise l'authentification inter-domaines Kerberos, spécifiez le nom du principal de l'utilisateur complet, y compris le nom du domaine. Par exemple : sysadmin@COMPANY.COM

UpdateKerberosConfig

Utilisez la commande UpdateKerberosConfig pour corriger le nom du domaine ou le nom du domaine de service dans la configuration de Informatica. Vous pouvez modifier le domaine d'utilisateur auquel les utilisateurs du domaine Informatica appartiennent. Vous pouvez modifier le domaine de service auquel les services du domaine Informatica appartiennent.

Remarque: Cette commande ne modifie pas la configuration Kerberos. Vous ne pouvez pas utiliser cette commande pour migrer des utilisateurs d'un domaine d'utilisateur ou d'un domaine de service vers un autre.

La commande UpdateKerberosConfig utilise la syntaxe suivante :

```
UpdateKerberosConfig
[<-ServiceRealmName|-srn> realm_name_of_node_spn]
[<-UserRealmName|-urn> realm_name_of_user_spn]
```

Le tableau suivant décrit les options et les arguments de la commande *infasetup* UpdateKerberosConfig :

Option	Argument	Description
-ServiceRealmName -srn	realm_name_of_node_s n	Facultatif. Nom du domaine Kerberos que le domaine utilise pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules. Pour configurer l'authentification inter-domaines Kerberos, spécifiez le nom de chaque domaine Kerberos que le domaine utilise pour l'authentification des utilisateurs, séparé par une virgule. Par exemple : COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple, spécifiez la valeur suivante afin d'inclure tous les domaines qui incluent le nom EAST.COMPANY.COM : *EAST.COMPANY.COM
-UserRealmName -urn	realm_name_of_user_s n	Facultatif. Nom du domaine Kerberos que le domaine utilise pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules. Pour configurer l'authentification inter-domaines Kerberos, spécifiez le nom de chaque domaine Kerberos que le domaine utilise pour l'authentification des utilisateurs, séparé par une virgule. Par exemple : COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple, spécifiez la valeur suivante afin d'inclure tous les domaines qui incluent le nom EAST.COMPANY.COM : *EAST.COMPANY.COM

updateMitKerberosLinkage

Configure les clients de base de données personnalisée et le domaine Informatica pour utiliser les bibliothèques Kerberos personnalisées spécifiées au lieu des bibliothèques par défaut qu'Informatica utilise.

Pour utiliser les bibliothèques Kerberos personnalisées, procédez comme suit :

1. Copiez les bibliothèques Kerberos personnalisées que vous souhaitez utiliser sur chaque nœud, ou dans un emplacement auquel tous les nœuds du domaine Informatica peuvent accéder.
2. Arrêtez le domaine.
3. Exécutez la commande *infasetup updateMitKerberosLinkage* sur chaque nœud du domaine.
4. Après avoir exécuté la commande sur tous les nœuds du domaine, démarrez le domaine.

La commande `updateMitKerberosLinkage` utilise la syntaxe suivante :

```
updateMitKerberosLinkage  
  
<-useKerberos|-krb> true|false  
  
[<-mitKerberosDirectory|-mkd> kerberos_library_directory]
```

Le tableau suivant décrit les options et arguments de la commande `infasetup updateMitKerberosLinkage` :

Option	Argument	Description
-useKerberos -krb	true false	<p>Requis. Valeur booléenne. Si le domaine Informatica utilise l'authentification Kerberos, définissez cette valeur sur true. Si elle est définie sur true, les processus Informatica effectuent les appels Kerberos auprès des bibliothèques Kerberos par défaut ou des bibliothèques dans le répertoire spécifié avec l'option -mkd.</p> <p>Si le domaine Informatica n'utilise pas l'authentification Kerberos, définissez cette valeur sur false. Si elle est définie sur false, Informatica ne charge pas les bibliothèques Kerberos. Les clients tiers, comme les clients de base de données, effectuent les appels auprès des bibliothèques spécifiées dans le répertoire spécifié avec l'option -mkd.</p>
-mitKerberosDirectory -mkd	spn_nœud_répertoire_bibliothèque_kerberos	<p>Facultatif. Répertoire contenant les bibliothèques Kerberos MIT personnalisées. Le répertoire doit contenir les fichiers des bibliothèques. Vous ne pouvez pas utiliser de liens symboliques.</p> <p>Si l'option -krb est définie sur true, assurez-vous que le numéro de version des bibliothèques Kerberos personnalisées que vous souhaitez utiliser est le même que celui des bibliothèques Kerberos qu'Informatica utilise par défaut.</p> <p>S'il existe plusieurs versions de la même bibliothèque, toutes les versions doivent être de la même taille et avoir la même somme de contrôle. Par exemple, si le répertoire contient deux versions de libkrb5, comme libkr5.so.3 et libkrb5.so, les deux bibliothèques doivent avoir la même valeur de taille de fichier et de somme de contrôle.</p> <p>Si le répertoire spécifié est vide, la commande supprime toutes les bibliothèques Kerberos personnalisées du domaine Informatica.</p>

UpdatePasswordComplexityConfig

Mettez à jour la configuration de la complexité du mot de passe pour le domaine.

La syntaxe de la commande `infasetup UpdatePasswordComplexityConfig` est la suivante :

```
UpdatePasswordComplexityConfig  
<-EnablePasswordComplexity|-pc> enable_password_complexity
```

Le tableau suivant décrit les options et arguments d'infasetup UpdatePasswordComplexityConfig :

Option	Argument	Description
-EnablePasswordComplexity -pc	enable_password_complexity	<p>Facultatif. Activez la complexité du mot de passe pour valider le niveau de sécurité correspondant. Cette option est désactivée par défaut.</p> <p>Pour un compte utilisateur natif, si vous activez la complexité du mot de passe, utilisez les directives suivantes lorsque vous créez ou modifiez un mot de passe :</p> <ul style="list-style-type: none"> - Le mot de passe doit contenir au moins huit caractères. - Il doit être composé d'un caractère alphabétique, d'un caractère numérique et d'un caractère non alphanumérique, tels que : <p>! \ " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { } ~</p> <p>Lorsque vous utilisez des caractères spéciaux dans un mot de passe, il arrive que l'interpréteur de commandes les lise différemment. Par exemple, \$ est interprété comme une variable. Dans ce cas, utilisez un caractère d'échappement pour échapper le caractère spécial.</p>

UpdateDomainSamlConfig

Active ou désactive l'authentification SAML (Secure Assertion Markup Language) pour les applications Web Informatica dans un domaine Informatica. Vous pouvez également utiliser la commande pour mettre à jour l'URL du fournisseur d'identité et spécifier la différence temporelle autorisée entre l'horloge système du fournisseur d'identité et celle du nœud principal de passerelle.

Exécutez la commande sur chaque nœud de passerelle du domaine Informatica. Avant d'exécuter la commande, arrêtez le domaine.

La commande infasetup updateDomainSamlConfig utilise la syntaxe suivante :

```
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]
```

Le tableau suivant décrit les options et arguments de la commande `infasetup updateDomainSamlConfig` :

Option	Description
-EnableSaml -saml	Facultatif. Active ou désactive l'authentification SAML dans le domaine Informatica. Définissez cette valeur sur True pour activer l'authentification SAML dans le domaine Informatica. La valeur par défaut est False.
-idpUrl -iu	Requis si l'option -saml est définie sur true. Spécifiez l'URL du fournisseur d'identité du domaine. Vous devez spécifier la chaîne complète de l'URL.
-ServiceProviderId -spid	Facultatif. Nom d'approbation de la partie de confiance ou identificateur de fournisseur de services pour le domaine, tel que défini dans le fournisseur d'identité. Si vous avez spécifié « Informatica » comme nom de tiers de confiance dans AD FS, vous n'avez pas besoin de spécifier une valeur.
-ClockSkewTolerance -cst	Facultatif. Différence temporelle autorisée entre l'horloge système du fournisseur d'identité et celle du nœud principal de passerelle. La durée de vie des jetons SAML émis par le fournisseur d'identité est définie selon l'horloge système de l'hôte du fournisseur d'identité. La durée de vie d'un jeton SAML émis par le fournisseur d'identité est valide si l'heure de début ou l'heure de fin définie dans le jeton est comprise dans le nombre de secondes spécifié de l'horloge système du nœud principal de passerelle. Les valeurs doivent être comprises entre 0 et 600 secondes. La valeur par défaut est 120 secondes.
-SamlAssertionSigned -sas	Facultatif. Définissez cette option sur TRUE pour activer la signature d'assertion par le fournisseur d'identité. La valeur par défaut est FALSE.
-AssertionSigningCertificateAlias -asca	Obligatoire si SamlAssertionSigned est défini sur TRUE. Nom d'alias spécifié lors de l'importation du certificat de signature d'assertion du fournisseur d'identité dans le fichier truststore utilisé pour l'authentification SAML.
-AuthnContextComparsion -acc	Spécifie la méthode de comparaison utilisée pour évaluer l'instruction d'autorisation demandée. Un des éléments suivants : <ul style="list-style-type: none"> - MINIMUM. Le contexte d'authentification dans l'instruction d'authentification doit correspondre exactement à au moins un des contextes d'authentification spécifiés. - MAXIMUM. Le contexte d'authentification dans l'instruction d'authentification doit être au moins aussi fort (tel que jugé par le répondeur) que l'un des contextes d'authentification spécifiés. - BETTER. Le contexte d'authentification dans l'instruction d'authentification doit être plus fort (tel que jugé par le répondeur) que l'un des contextes d'authentification spécifiés. - EXACT. Le contexte d'authentification dans l'instruction d'authentification doit être aussi fort que possible (tel que jugé par le répondeur), sans dépasser la force d'au moins un des contextes d'authentification spécifiés. La valeur par défaut est Exact.
-AuthnContextClassRef -accr	Classe du contexte d'authentification. Un des suivants : <ul style="list-style-type: none"> - PASSWORD - PASSWORDPROTECTEDTRANSPORT
-SignSamlRequest -ssr	Défini sur True pour activer la signature de demande La valeur par défaut est False.

Option	Description
-RequestSigningPrivateKeyAlias -rspa	Requis si vous activez la demande signée. Nom d'alias de la clé privée qu'Informatica utilise pour signer la demande. Cette clé privée réside dans le keystore du nœud de passerelle. La clé publique correspondante (généralement un certificat) doit être importée vers le fournisseur d'identité.
-RequestSigningPrivateKeyPassword -rspp	Mot de passe en texte brut de la clé privée qu'Informatica utilise pour signer la demande. La valeur par défaut est le mot de passe de la clé privée présente dans le fichier keystore <Informatica home>\services\shared\security\infa_keystore.jks avec l'alias « Informatica LLC ».
-RequestSigningAlgorithm -rsa	Requis si vous activez la demande signée. Algorithme utilisé pour signer la demande. Un des suivants : <ul style="list-style-type: none"> - RSA_SHA256 - DSA_SHA1 - DSA_SHA256 - RSA_SHA1 - RSA_SHA224 - RSA_SHA384 - RSA_SHA512 - ECDSA_SHA1 - ECDSA_SHA224 - ECDSA_SHA256 - ECDSA_SHA384 - ECDSA_SHA512 - RIPEMD160 - RSA_MD5
-SamlResponseSigned -srs	Définissez cette option sur True pour spécifier si l'IDP signe la réponse SAML. Remarque: Lorsqu'elle est définie sur TRUE, l'administrateur IDP doit configurer le fournisseur d'identité pour signer la réponse. La valeur par défaut est False.
-ResponseSigningCertificateAlias -rsca	Requis si vous activez la réponse signée. Nom d'alias du certificat dans le truststore SAML du nœud de passerelle à utiliser pour vérifier la signature.
-SamlAssertionEncrypted -sae	Définissez cette option sur True pour spécifier si l'IDP chiffre l'assertion. Remarque: Lorsqu'elle est définie sur True, l'administrateur IDP doit configurer le fournisseur d'identité pour chiffrer l'assertion. La valeur par défaut est False.
-EncryptedAssertionPrivateKeyAlias -espa	Nom d'alias de la clé privée présente dans le keystore SAML du nœud de passerelle. La clé privée est utilisée pour chiffrer l'assertion. L'administrateur IDP doit importer la clé publique correspondante (généralement un certificat).
-EncryptedAssertionPrivateKeyPassword -espp	Mot de passe en texte brut. La valeur par défaut est le mot de passe de la clé privée présente dans le fichier keystore <Informatica home>\services\shared\security\infa_keystore.jks avec l'alias « Informatica LLC ».

UpdateWorkerNode

Met à jour les informations de connectivité pour un nœud de travail sur l'ordinateur actuel. Avant de mettre à jour le nœud de travail, exécutez la commande `infacmd isp ShutDownNode` pour arrêter le nœud.

La syntaxe de la commande `UpdateWorkerNode` est la suivante :

```
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]
```

Le tableau suivant décrit les options et arguments d'*infasetup* `UpdateWorkerNode` :

Option	Description
-DomainName -dn	Facultatif. Nom du domaine.
-NodeName -nn	Facultatif. Nom du nœud. Les noms de nœud doivent avoir une longueur comprise entre 1 et 79 caractères et ne peuvent contenir ni des espaces, ni les caractères suivants : \ / * ? < > "
-NodeAddress -na	Facultatif. Nom d'hôte et numéro de port de la machine hébergeant le nœud. Choisissez un numéro de port disponible.
-ServiceManagerPort -sp	Facultatif. Numéro de port utilisé par le gestionnaire de service pour écouter les demandes de connexions entrantes.

Option	Description
-EnableTLS -tls	<p>Facultatif. Configure la communication sécurisée des services dans le domaine Informatica.</p> <p>Si vous utilisez les certificats SSL par défaut fournis par Informatica, vous n'avez pas besoin de spécifier les options keystore et truststore. Si vous n'utilisez pas le certificat SSL par défaut, vous devez spécifier les options keystore et truststore. Les valeurs valides sont True ou False. La valeur par défaut est false. Si vous spécifiez l'option -tls sans valeur, le domaine Informatica utilise la communication sécurisée entre les services.</p> <p>Pour activer la communication sécurisée pour les services ou applications Web associés, tels que l'outil Administrator tool, l'outil Analyst tool ou le hub de services Web, configurez la communication sécurisée séparément dans les applications.</p>
-NodeKeystore- -nk	<p>Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Requis si vous utilisez vos certificats SSL. Répertoire contenant les fichiers keystore. Le domaine Informatica requiert les certificats SSL au format PEM et dans des fichiers Java Keystore (JKS). Le répertoire doit contenir les fichiers keystore aux formats PEM et JKS.</p> <p>Les fichiers keystore doivent être nommés infa_keystore.jks et infa_keystore.pem. Si le fichier keystore que vous recevez de l'autorité de certification (CA) a un nom différent, vous devez le renommer infa_keystore.jks et infa_keystore.pem.</p> <p>Vous devez utiliser le même fichier keystore pour tous les nœuds du domaine.</p>
-NodeKeystorePass -nkp	<p>Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Requis si vous utilisez vos certificats SSL. Mot de passe pour le fichier keystore infa_keystore.jks.</p>
-NodeTruststore -nt	<p>Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Répertoire contenant les fichiers truststore. Le domaine Informatica requiert les certificats SSL au format PEM et dans des fichiers Java Keystore (JKS). Le répertoire doit contenir les fichiers truststore aux formats PEM et JKS.</p> <p>Les fichiers truststore doivent être nommés infa_truststore.jks et infa_truststore.pem. Si le fichier truststore que vous recevez de l'autorité de certification (CA) a un nom différent, vous devez le renommer infa_truststore.jks et infa_truststore.pem.</p>
-NodeTruststorePass -ntp	<p>Facultatif si vous utilisez les certificats SSL par défaut depuis Informatica. Requis si vous utilisez vos certificats SSL. Mot de passe du fichier infa_truststore.jks.</p>
-CipherWhiteList -cwl	<p>Facultatif. Liste séparée par des virgules de suites de chiffrement JSSE que vous souhaitez ajouter à la liste effective.</p> <p>Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.</p>
-CipherBlackList -cbl	<p>Facultatif. Liste séparée par des virgules de suites de chiffrement JSSE que vous souhaitez supprimer de la liste effective.</p> <p>Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.</p>
-CipherWhiteListFile -cwlf	<p>Facultatif. Nom de fichier absolu du fichier en texte brut qui contient une liste de suites de chiffrement séparée par des virgules à ajouter à la liste effective.</p> <p>Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.</p>
-CipherBlackListFile -cblf	<p>Facultatif. Nom de fichier absolu du fichier en texte brut qui contient une liste de suites de chiffrement séparée par des virgules que vous souhaitez supprimer de la liste effective.</p> <p>Remarque: Elle doit contenir au moins une suite de chiffres JRE ou OpenSSL valide.</p>

Option	Description
-EnableKerberos -krb	Facultatif. Configure le domaine Informatica pour qu'il utilise l'authentification Kerberos. Les valeurs valides sont True ou False. Si la valeur est True, le domaine utilise l'authentification Kerberos et vous ne pouvez plus changer le mode d'authentification. Après avoir activé l'authentification Kerberos, vous ne pouvez pas la désactiver. La valeur par défaut est False. Si vous spécifiez l'option -krb sans valeur, le domaine Informatica utilise l'authentification Kerberos.
-ServiceRealmName -srn	Facultatif. Nom du domaine Kerberos que le domaine utilise pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules. Pour configurer l'authentification inter-domaines Kerberos, spécifiez le nom de chaque domaine Kerberos que le domaine utilise pour l'authentification des utilisateurs, séparé par une virgule. Par exemple : COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple, spécifiez la valeur suivante afin d'inclure tous les domaines qui incluent le nom EAST.COMPANY.COM : *EAST.COMPANY.COM
-UserRealmName -urn	Facultatif. Nom du domaine Kerberos que le domaine utilise pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules. Pour configurer l'authentification inter-domaines Kerberos, spécifiez le nom de chaque domaine Kerberos que le domaine utilise pour l'authentification des utilisateurs, séparé par une virgule. Par exemple : COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple, spécifiez la valeur suivante afin d'inclure tous les domaines qui incluent le nom EAST.COMPANY.COM : *EAST.COMPANY.COM
-KeysDirectory -kd	Facultatif. Répertoire dans lequel sont stockés tous les fichiers Keytab et la clé de cryptage pour le domaine Informatica. La valeur par défaut est <InformaticaInstallationDir>/isp/config/keys.
-HttpsPort -hs	Facultatif. Numéro de port pour sécuriser la connexion à l'outil Administrator tool. Définissez ce numéro de port si vous souhaitez configurer HTTPS pour un nœud.
-KeystoreFile -kf	Facultatif. Le fichier keystore contenant les clés et les certificats est requis si vous utilisez le protocole de sécurité SSL.
-KeystorePass -kp	Facultatif. Mot de passe en texte brut du fichier keystore. Vous pouvez définir un mot de passe avec l'option -kp ou la variable d'environnement INFA_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -kp est prioritaire.
-GatewayAddress -dg	Requis. Nom de machine et numéro de port de l'hôte de passerelle.
-UserName -un	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Description
-SecurityDomain -sdn	<p>Nom du domaine de sécurité que vous voulez créer et auquel l'utilisateur du domaine appartient. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Vous pouvez spécifier une valeur pour -sdn ou utiliser la valeur par défaut selon le mode d'authentification :</p> <ul style="list-style-type: none"> - Requis si le domaine utilise l'authentification LDAP. La valeur par défaut est Natif. Pour travailler avec l'authentification LDAP, vous devez spécifier la valeur pour -sdn. - Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. La valeur par défaut est natif pour l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Password -pd	<p>Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.</p>
-MinProcessPort -mi	<p>Requis. Numéro de port minimal pour les processus de service d'application exécutés sur le nœud.</p>
-MaxProcessPort -ma	<p>Requis. Numéro de port maximal pour les processus de service d'application exécutés sur le nœud.</p>
-ServerPort -sv	<p>Facultatif. Numéro de port TCP/IP utilisé par le gestionnaire de service. Ce port permet au gestionnaire de service d'écouter les commandes d'arrêt en provenance des composants du domaine. Définissez ce numéro de port si vous avez plusieurs nœuds sur une machine ou si le numéro de port par défaut est utilisé. La valeur par défaut est le numéro de port du nœud plus un.</p>
-BackupDirectory -bd	<p>Facultatif. Répertoire de stockage des fichiers de sauvegarde du référentiel. Le nœud doit avoir accès au répertoire.</p>
-ErrorLogLevel -el	<p>Facultatif. Niveau de gravité des événements de journal dans le journal de domaine. La valeur par défaut est Informations.</p>
-ResourceFile -rf	<p>Requis. Fichier contenant la liste des ressources disponibles pour le nœud. Utilisez le fichier nodeoptions.xml situé à l'emplacement suivant : <code><Informatica installation directory>/isp/bin</code></p>
-EnableSaml -saml	<p>Facultatif. Active ou désactive l'authentification SAML dans le domaine Informatica. Définissez cette valeur sur True pour activer l'authentification SAML dans le domaine Informatica. La valeur par défaut est False.</p>
-SamlKeyStoreDir -skd	<p>Facultatif. Répertoire contenant le fichier keystore personnalisé requis pour utiliser l'authentification SAML sur le nœud de passerelle. Spécifiez le répertoire uniquement, pas le chemin d'accès complet au fichier.</p>
-SamlKeyStorePassword -skp	<p>Obligatoire si vous utilisez un fichier keystore personnalisé pour l'authentification SAML. Mot de passe du keystore SAML. *</p>

Option	Description
-GatewayAddress -dg	Requis. Nom de machine et numéro de port de l'hôte de passerelle.
-UserName -un	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option -un ou la variable d'environnement INFA_DEFAULT_DOMAIN_USER. Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option -un est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.
-SecurityDomain -sdn	Nom du domaine de sécurité que vous voulez créer et auquel l'utilisateur du domaine appartient. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Vous pouvez spécifier une valeur pour -sdn ou utiliser la valeur par défaut selon le mode d'authentification : <ul style="list-style-type: none"> - Obligatoire si le domaine utilise l'authentification LDAP. La valeur par défaut est Native. Pour travailler avec l'authentification LDAP, vous devez spécifier la valeur pour -sdn. - Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. La valeur par défaut est natif pour l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-Password -pd	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServerPort -sv	Facultatif. Numéro de port TCP/IP utilisé par le gestionnaire de service. Le gestionnaire de service utilise ce port pour écouter les commandes d'arrêt des composants PowerCenter. Définissez ce numéro de port si vous avez plusieurs nœuds sur une machine ou si le numéro de port par défaut est utilisé.
-resetHostPort -rst	Obligatoire si vous spécifiez l'option NodeAddress ou ServiceManager. Réinitialise le numéro de port hôte.
-SystemLogDirectory -sld	Facultatif. Chemin du répertoire pour stocker les fichiers journaux système. La valeur par défaut est <INFA_home>/logs.
* Remarque : si vous exécutez actuellement des scripts qui utilisent cette commande pour activer un keystore personnalisé pour l'authentification SAML, vous devez les mettre à jour afin d'y inclure cette option.	

upgradeDomainMetadata

Met à jour les métadonnées du domaine. Avant de mettre à jour le domaine, exécutez la commande `infacmd isp ShutDownNode` pour arrêter le nœud.

La syntaxe de la commande `upgradeDomainMetadata` est la suivante :

```
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)]
```

Le tableau suivant décrit les options et les arguments de la commande `infasetup upgradeDomainMetadata` :

Option	Description
-PreviousInfaHome -ph	Requis. Chemin du répertoire de base Informatica précédent.
-DatabaseAddress -da	Obligatoire si vous n'utilisez pas l'option -DatabaseConnectionString (-cs). Nom et numéro du port de la machine hébergeant la base de données de configuration du domaine.
-DatabaseUserName -du	Obligatoire si vous n'utilisez pas l'option -TrustedConnection (-tc). Compte de la base de données qui contient les informations de configuration du domaine.
-DatabasePassword -dp	Mot de passe de la base de données de configuration du domaine correspondant à l'utilisateur de la base de données. Si vous omettez cette option, <i>infasetup</i> utilisera le mot de passe spécifié dans la variable d'environnement <code>INFA_DEFAULT_DATABASE_PASSWORD</code> . Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, vous devez entrer un mot de passe à l'aide de cette option.
-DatabaseType -dt	Requis. Type de base de données contenant les métadonnées de configuration du domaine. Les types de base de données sont les suivants : <ul style="list-style-type: none">- db2- oracle- mssqlserver- sybase- postgresql
-DatabaseServiceName -ds	Obligatoire si vous n'utilisez pas l'option -DatabaseConnectionString (-cs). Nom du service de base de données. Obligatoire pour les bases de données Oracle, IBM DB2 et Microsoft SQL Server. Entrez le SID pour Oracle, le nom du service pour IBM DB2 ou le nom de la base de données pour Microsoft SQL Server.

Option	Description
-Tablespace -ts	Obligatoire dans le cas d'une base de données IBM DB2. Nom de l'espace de table dans lequel se situent les tables de la base de données de configuration du domaine.
-SchemaName -sc	Facultatif. Nom du schéma Microsoft SQL Server. Entrez un nom de schéma si vous n'utilisez pas le schéma par défaut.
-TrustedConnection -tc	Facultatif. Connexion à la base de données Microsoft SQL Server via une connexion approuvée. L'authentification de confiance utilise les justificatifs d'identité de sécurité Windows de l'utilisateur en cours pour effectuer la connexion à Microsoft SQL Server.
-KeysDirectory -kd	Facultatif. Répertoire dans lequel sont stockés tous les fichiers Keytab et la clé de cryptage pour le domaine Informatica. La valeur par défaut est <code><InformaticaInstallationDir>/isp/config/keys</code> .
-DatabaseTlsEnabled -dbtls	Facultatif. Indique si la base de données du domaine Informatica est sécurisée avec le protocole TLS ou SSL. Définissez cette option sur True pour la base de données sécurisée. La valeur par défaut est false. Si vous spécifiez l'option -dbtls sans valeur, le domaine Informatica utilise la communication sécurisée avec la base de données du domaine Informatica.
-DatabaseTruststorePassword -dbtp	Facultatif. Mot de passe du fichier truststore de la base de données sécurisée.
-DatabaseTruststoreLocation -dbtl	Facultatif. Chemin et nom du fichier truststore du nœud de passerelle.
-SingletonServiceParameters -ssp	Facultatif. Mettez à niveau les paramètres du service à l'aide de l'une des options suivantes : <ul style="list-style-type: none"> - SystemServicesFolderName - SchedulerService - ResourceManager - EmailService Syntaxe : <code>infasetup upgradeDomainMetadata -ssp <option>=<value></code>

UpgradeGatewayNodeMetadata

Met à jour les métadonnées pour un nœud de passerelle sur la machine actuelle. Avant de mettre à jour le nœud de passerelle, exécutez la commande `infacmd isp ShutDownNode` pour arrêter le nœud.

La syntaxe de la commande `UpgradeGatewayNodeMetadata` est la suivante :

```
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]

```

Le tableau suivant décrit les options et les arguments de la commande *infasetup*
UpgradeGatewayNodeMetadata :

Option	Description
-LogServiceDirectory -ld	Requis. Chemin du répertoire partagé utilisé par le gestionnaire de journaux pour stocker des fichiers d'événements de journal. Vérifiez que -ld ne correspond pas à la valeur--sld spécifiée ni ne la contient.
-SystemLogDirectory -sld	Facultatif. Chemin du répertoire pour stocker les fichiers journaux système. Vérifiez que -ld ne correspond pas à la valeur--sld spécifiée ni ne la contient. La valeur par défaut est <INFA_home>/logs.
-HttpsPort -hs	Facultatif. Numéro de port utilisé par le nœud pour la communication entre l'outil Administrator tool et le Gestionnaire de service. Définissez ce numéro de port si vous souhaitez configurer HTTPS pour un nœud. Pour désactiver le support HTTPS pour un nœud, initialisez ce numéro à zéro.
-KeystoreFile -kf	Facultatif. Le fichier keystore contenant les clés et les certificats est requis si vous utilisez le protocole de sécurité SSL.
-KeystorePass -kp	Facultatif. Mot de passe en texte brut du fichier keystore. Vous pouvez définir un mot de passe avec l'option -kp ou la variable d'environnement INFA_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -kp est prioritaire.
-DatabaseAddress -da	Obligatoire si vous n'utilisez pas l'option -DatabaseConnectionString (-cs). Nom et numéro du port de la machine hébergeant la base de données de configuration du domaine.
-DatabaseConnectionString -cs	Obligatoire si vous n'utilisez pas les options -DatabaseAddress (-da) et --DatabaseServiceName (-ds). Chaîne de connexion utilisée pour se connecter à la base de données de configuration du domaine. La chaîne de connexion doit inclure l'hôte de la base de données, le port de la base de données et le nom du service de base de données. Placez la chaîne de connexion entre guillemets.
-DatabaseUserName -du	Obligatoire si vous n'utilisez pas l'option -TrustedConnection (-tc). Compte de la base de données qui contient les informations de configuration du domaine.
-DatabasePassword -dp	Mot de passe de la base de données de configuration du domaine correspondant à l'utilisateur de la base de données. Si vous omettez cette option, <i>infasetup</i> utilisera le mot de passe spécifié dans la variable d'environnement INFA_DEFAULT_DATABASE_PASSWORD. Dans le cas où aucune valeur n'est spécifiée dans la variable d'environnement, vous devez entrer un mot de passe à l'aide de cette option.

Option	Description
-DatabaseType -dt	Requis. Type de base de données contenant les métadonnées de configuration du domaine. Les types de base de données sont les suivants : <ul style="list-style-type: none"> - db2 - oracle - mssqlserver - sybase - postgresql
-DatabaseServiceName -ds	Obligatoire si vous n'utilisez pas l'option -DatabaseConnectionString (-cs). Nom du service de base de données. Obligatoire pour les bases de données Oracle, IBM DB2 et Microsoft SQL Server. Entrez le SID pour Oracle, le nom du service pour IBM DB2 ou le nom de la base de données pour Microsoft SQL Server.
-Tablespace -ts	Obligatoire dans le cas d'une base de données IBM DB2. Nom de l'espace de table dans lequel se situent les tables de la base de données de configuration du domaine.
-SchemaName -sc	Facultatif. Nom du schéma Microsoft SQL Server. Entrez un nom de schéma si vous n'utilisez pas le schéma par défaut.
-TrustedConnection -tc	Facultatif. Connexion à la base de données Microsoft SQL Server via une connexion approuvée. L'authentification de confiance utilise les justificatifs d'identité de sécurité Windows de l'utilisateur en cours pour effectuer la connexion à Microsoft SQL Server.
-PreviousInfraHome -ph	Requis. Chemin du répertoire de base Informatica précédent.
-KeysDirectory -kd	Facultatif. Répertoire dans lequel sont stockés tous les fichiers Keytab et la clé de cryptage pour le domaine Informatica. La valeur par défaut est <InformaticaInstallationDir>/isp/config/keys.
-DatabaseTlsEnabled -dbtls	Facultatif. Indique si la base de données du domaine Informatica est sécurisée avec le protocole TLS ou SSL. Définissez cette option sur True pour la base de données sécurisée. La valeur par défaut est false. Si vous spécifiez l'option -dbtls sans valeur, le domaine Informatica utilise la communication sécurisée avec la base de données du domaine Informatica.
-DatabaseTruststorePassword -dbtp	Facultatif. Mot de passe du fichier truststore de la base de données sécurisée.
-DatabaseTruststoreLocation -dbtl	Facultatif. Chemin et nom du fichier truststore du nœud de passerelle.

UnlockUser

Déverrouille un compte utilisateur natif ou LDAP. Lorsque vous déverrouiller un compte utilisateur natif, vous pouvez également fournir un nouveau mot de passe pour le compte.

Vous pouvez déverrouiller un compte utilisateur après avoir arrêté le domaine à partir du nœud de passerelle.

La syntaxe de la commande infasetup UnlockUser est la suivante :

```
UnlockUser

<-UserName|-un> user_name

[<-SecurityDomain|-sdn] security domain]

[<-NewPassword|-np] new_password]
```

Le tableau suivant décrit les options et arguments d'infasetup UnlockUser :

Option	Argument	Description
-UserName -un	user_name	Requis. Nom d'utilisateur du compte verrouillé. Cette valeur est sensible à la casse.
-SecurityDomain -sdn	domaine de sécurité	<p>Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse.</p> <p>Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.</p>
-NewPassword -np	new_password	<p>Facultatif. Nouveau mot de passe pour le compte natif verrouillé.</p> <p>Pour un compte utilisateur natif, si vous activez la complexité du mot de passe, utilisez les directives suivantes lorsque vous créez ou modifiez un mot de passe :</p> <ul style="list-style-type: none">- Le mot de passe doit contenir au moins huit caractères.- Il doit être composé d'un caractère alphabétique, d'un caractère numérique et d'un caractère non alphanumérique, tels que : <pre>! \ " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { } ~</pre> <p>Lorsque vous utilisez des caractères spéciaux dans un mot de passe, il arrive que l'interpréteur de commandes les lise différemment. Par exemple, \$ est interprété comme une variable. Dans ce cas, utilisez un caractère d'échappement pour échapper le caractère spécial.</p>

ValidateandRegisterFeature

Valide et enregistre la fonctionnalité dans le domaine.

La commande ValidateandRegisterFeature utilise la syntaxe suivante :

```
ValidateandRegisterFeature

<-FeatureFilename|-ff> feature_filename

<-IsUpgrade|-up> is_upgrade
```


Le tableau suivant décrit les options et les arguments ValidateandRegisterFeature de la commande *infasetup* :

Option	Argument	Description
-FeatureFilename -ff	feature_filename	Requis. Emplacement du fichier xml pour le plug-in.
-IsUpgrade -up	is_upgrade	Requis. Indique si vous souhaitez mettre à niveau le plug-in vers la version spécifiée dans le fichier de fonctionnalités. Les valeurs valides sont True et False. La valeur par défaut est True.

CHAPITRE 43

Référence de commande pmcmd

Ce chapitre comprend les rubriques suivantes :

- [Utilisation de pmcmd, 1335](#)
- [aborttask, 1340](#)
- [abortworkflow, 1342](#)
- [Connect, 1344](#)
- [Déconnecter, 1345](#)
- [Exit, 1345](#)
- [getrunningsessionsdetails, 1346](#)
- [GetServiceDetails, 1347](#)
- [getserviceproperties, 1349](#)
- [getsessionstatistics, 1350](#)
- [gettaskdetails, 1352](#)
- [getworkflowdetails, 1354](#)
- [help, 1357](#)
- [pingservice, 1358](#)
- [recoverworkflow, 1359](#)
- [scheduleworkflow, 1361](#)
- [SetFolder, 1362](#)
- [SetNoWait, 1363](#)
- [SetWait, 1363](#)
- [ShowSettings, 1363](#)
- [StartTask, 1364](#)
- [StartWorkflow, 1367](#)
- [StopTask, 1370](#)
- [StopWorkflow, 1372](#)
- [UnscheduleWorkflow, 1374](#)
- [UnsetFolder, 1375](#)
- [Version, 1376](#)
- [WaitTask, 1376](#)
- [WaitWorkflow, 1378](#)

Utilisation de pmcmd

pmcmd est un programme servant à communiquer avec le service d'intégration. Avec *pmcmd*, vous pouvez effectuer certaines des tâches également réalisables dans le gestionnaire de flux de travail, telles que le démarrage et l'arrêt des flux de travail et des sessions.

Utilisez *pmcmd* dans les modes suivants :

- **Mode ligne de commande.** Vous invoquez et vous quittez *pmcmd* à chaque exécution de commande. Vous pouvez écrire des scripts pour planifier les flux de travail avec la syntaxe de ligne de commande. Chaque commande passée en mode ligne de commande doit inclure les informations de connexion au service d'intégration.
- **Mode interactif.** Vous établissez et maintenez une connexion active au service d'intégration. Ceci vous permet d'émettre une série de commandes.

Vous pouvez utiliser des variables d'environnement pour les noms d'utilisateur et les mots de passe avec *pmcmd*. Vous pouvez aussi utiliser les variables d'environnement pour personnaliser la manière dont *pmcmd* affiche la date et l'heure sur la machine qui exécute le processus de service d'intégration. Avant d'utiliser *pmcmd*, configurez ces variables sur la machine qui exécute le processus de service d'intégration. Les variables d'environnement s'appliquent aux commandes *pmcmd* qui s'exécutent sur le nœud.

Remarque: Si le domaine est un domaine multiversions, exécutez *pmcmd* depuis le répertoire d'installation de la version du service d'intégration.

Exécution de commandes en mode ligne de commande

Le mode ligne de commande appelle et quitte *pmcmd* chaque fois que vous exécutez une commande. Le mode ligne de commande est utile si vous souhaitez exécuter des commandes *pmcmd* via des fichiers de lots, des scripts ou d'autres programmes.

Utilisez des commandes *pmcmd* avec les outils de planification du système d'exploitation tels que *cron*, ou vous pouvez incorporer des commandes *pmcmd* dans le shell ou des scripts Perl.

Lorsque vous utilisez *pmcmd* en mode ligne d'invite, vous saisissez des informations de connexion comme le nom de domaine, le nom de service d'intégration, le nom d'utilisateur et le mot de passe. Par exemple, pour démarrer le flux de travail « wf_SalesAvg » dans le dossier « SalesEast », utilisez la syntaxe suivante :

```
pmcmd startworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f SalesEast  
wf_SalesAvg
```

L'utilisateur, seller3, avec le mot de passe « jackson » envoie la requête de lancement du flux de travail.

Si vous omettez ou saisissez de manière incorrecte l'une des options obligatoires, la commande échoue et *pmcmd* renvoie un code de retour différent de zéro. Pour plus d'informations sur tous les codes de retour, consultez ["codes de retour pmcmd" à la page 1336](#).

Pour exécuter des commandes *pmcmd* en mode ligne de commande :

1. À l'invite de commande, passez au répertoire abritant l'exécutable *pmcmd*.
Par défaut, le programme d'installation de PowerCenter installe *pmcmd* dans le répertoire \server\bin.
2. Entrez *pmcmd* suivi du nom de commande et de ses options et arguments :

```
pmcmd command_name [-option1] argument_1 [-option2] argument_2...
```

codes de retour pmcmd

En mode ligne de commande, *pmcmd* indique la réussite ou l'échec d'une commande à l'aide d'un code de retour. Le code de retour « 0 » indique que la commande a réussi. Tout autre code de retour indique que la commande a échoué.

Utilisez la commande DOS ou UNIX « echo » immédiatement après avoir exécuté une commande *pmcmd* pour voir le code de retour de cette commande :

- Dans un shell DOS : `echo %ERRORLEVEL%`
- Dans un shell UNIX Bourne ou Korn : `echo $?`
- Dans un shell C UNIX : `echo $status`

Le tableau suivant décrit les codes de retour pour *pmcmd* :

Code	Description
0	Pour toutes les commandes, une valeur de retour de zéro indique que la commande a été correctement exécutée. Vous pouvez exécuter les commandes suivantes en mode attente ou nowait : starttask, startworkflow, aborttask et abortworkflow. Si vous exécutez une commande en mode attente, une valeur de retour de zéro indique que la commande a été correctement exécutée. Si vous exécutez une commande en mode nowait, une valeur de retour de zéro indique que la requête a été correctement transmise au service d'intégration et qu'il a confirmé la requête.
1	Le service d'intégration n'est pas disponible ou <i>pmcmd</i> ne peut pas se connecter à ce service. Un problème est survenu avec le nom d'hôte TCP/IP, le numéro de port ou le réseau.
2	Le nom de tâche, le nom de flux de travail ou le nom de dossier n'existent pas.
3	Une erreur s'est produite lors du démarrage ou de l'exécution du flux de travail ou de la tâche.
4	Erreur d'utilisation. Vous avez passé les mauvaises options à la commande <i>pmcmd</i> .
5	Une erreur <i>pmcmd</i> interne s'est produite. Contactez le service clientèle international d'Informatica.
7	Vous avez utilisé un nom d'utilisateur ou un mot de passe non valides.
8	Vous ne disposez pas des autorisations ou des privilèges nécessaires pour effectuer cette tâche.
9	La connexion au service d'intégration a dépassé le délai lors de l'envoi de la requête.
12	Le service d'intégration ne peut pas démarrer la récupération, car la session ou le flux de travail sont planifiés et attendent un événement, en attente, en initialisation, en abandon, en cours d'arrêt, désactivé ou en cours d'exécution.
13	La variable d'environnement de nom d'utilisateur est définie sur une valeur vide.
14	La variable d'environnement de mot de passe est définie sur une valeur vide.
15	La variable d'environnement de nom d'utilisateur est absente.
16	La variable d'environnement de mot de passe est absente.
17	Le fichier de paramètres n'existe pas.
18	Le service d'intégration a trouvé le fichier de paramètres, mais il ne contenait pas les valeurs initiales pour la session paramètres, tels que \$input ou \$output.

Code	Description
19	Le service d'intégration ne peut pas reprendre la session, car le flux de travail est configuré de façon à s'exécuter en continu.
20	Une erreur de référentiel s'est produite. Assurez-vous que le service de référentiel et la base de données sont en cours d'exécution et que le nombre de connexions à la base de données n'est pas dépassé.
21	Le service d'intégration est en cours de fermeture et il n'accepte plus de nouvelles requêtes.
22	Le service d'intégration ne peut pas trouver d'instance unique du flux de travail ou de la session que vous avez spécifiés. Entrez à nouveau la commande avec le nom de dossier et le nom de flux de travail.
23	Aucune donnée disponible pour la requête.
24	Mémoire épuisée.
25	La commande est annulée.

Exécution de commandes en mode interactif

Utilisez *pmcmd* en mode interactif pour démarrer et arrêter les flux de travail et les sessions sans créer de script. Lorsque vous utilisez le mode interactif, vous saisissez des informations de connexion comme le nom de domaine, le nom de service d'intégration, le nom d'utilisateur et le mot de passe. Vous pouvez exécuter les commandes suivantes sans entrer les informations de connexion pour chaque commande.

Par exemple, les commandes suivantes appellent le mode interactif, établissent une connexion au service d'intégration « MyIntService » et démarrent les flux de travail « wf_SalesAvg » et « wf_SalesTotal » dans le dossier « SalesEast » :

```
pmcmd
pmcmd> connect -sv MyIntService -d MyDomain -u seller3 -p jackson
pmcmd> setfolder SalesEast
pmcmd> startworkflow wf_SalesAvg
pmcmd> startworkflow wf_SalesTotal
```

Pour exécuter des commandes *pmcmd* en mode interactif :

1. À l'invite de commande, passez au répertoire abritant l'exécutable *pmcmd*.
Par défaut, le programme d'installation de PowerCenter installe pmcmd dans le répertoire \server\bin.
2. À l'invite de commande, saisissez *pmcmd*.
Ceci démarre *pmcmd* en mode interactif et affiche l'invite *pmcmd >*. Vous ne devez pas saisir *pmcmd* avant chaque commande en mode interactif.
3. Entrez les informations de connexion pour le domaine et le service d'intégration. Par exemple :

```
connect -sv MyIntService -d MyDomain -u seller3 -p jackson
```
4. Saisissez une commande et ses options et arguments au format suivant :

```
command_name [-option1] argument_1 [-option2] argument_2...
```

pmcmd exécute la commande et affiche l'invite à nouveau.
5. Saisissez *exit* pour terminer la session interactive.

Paramètres par défaut

Une fois que vous vous connectez à un service d'intégration à l'aide de *pmcmd*, vous pouvez désigner des dossiers ou conditions par défaut à utiliser chaque fois que le service d'intégration exécute une commande. Par exemple, si vous souhaitez émettre une série de commandes ou de tâches dans le même dossier, indiquez le nom du dossier avec la commande *setfolder*. Toutes les commandes suivantes utiliseront ce dossier comme valeur par défaut.

Le tableau suivant décrit les commandes à utiliser pour définir la valeur par défaut des commandes suivantes :

Commande	Description
<i>setfolder</i>	Désigne le dossier par défaut dans lequel vous souhaitez exécuter toutes les commandes suivantes.
<i>setnowait</i>	Exécute les commandes suivantes en mode <i>nowait</i> . L'invite <i>pmcmd</i> est disponible après que le service d'intégration ait reçu la commande précédente. Le mode <i>nowait</i> est le mode par défaut.
<i>setwait</i>	Exécute les commandes suivantes en mode attente. L'invite de commande <i>pmcmd</i> est disponible une fois que le service d'intégration a terminé la commande précédente.
<i>unsetfolder</i>	Inverse la commande <i>setfolder</i> .

Vous pouvez utiliser la commande *pmcmd ShowSettings* pour afficher les paramètres par défaut.

Exécution en mode attente

Vous pouvez exécuter la commande *pmcmd* en mode *wait* ou *nowait*. En mode *wait*, *pmcmd* revient à l'invite de commande ou au shell une fois la commande terminée. Vous ne pouvez pas exécuter les commandes suivantes tant que la commande précédente n'est pas terminée.

Par exemple, si vous entrez la commande suivante, *pmcmd* démarre le flux de travail « *wf_SalesAvg* » et ne renvoie pas l'invite tant que le flux de travail n'a pas terminé :

```
pmcmd startworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f SalesEast -  
wait wf_SalesAvg
```

En mode *nowait*, *pmcmd* revient immédiatement à l'invite de commande ou au shell. Vous n'avez pas besoin d'attendre qu'une commande se termine pour exécuter la commande suivante.

Par exemple, si vous entrez les commandes suivantes, *pmcmd* démarre le flux de travail « *wf_SalesTotal* », même si le flux de travail « *wf_SalesAvg* » est toujours en cours d'exécution :

```
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
```

Par défaut, *pmcmd* exécute les commandes en mode *nowait*.

Vous pouvez configurer le mode attente lorsque vous exécutez en ligne de commande ou mode interactif. En ligne de commande, utilisez l'option *-wait* pour exécuter une commande en mode attente. En mode interactif, utilisez la commande *setwait* ou *setnowait* avant de saisir les commandes suivantes.

Création de scripts de commandes *pmcmd*

Lorsque vous utilisez la commande *pmcmd*, vous pouvez utiliser régulièrement des commandes avec des options et des arguments spécifiques. Par exemple, vous pouvez utiliser la commande *pmcmd* pour contrôler

le statut du service d'intégration. Dans ce cas, vous pouvez créer un fichier de script ou de lots qui appelle une ou plusieurs commandes *pmcmd*, y compris leurs options et arguments.

Vous pouvez exécuter des scripts en mode ligne de commande. Vous ne pouvez pas exécuter les scripts *pmcmd* en mode interactif.

Par exemple, le script shell UNIX suivant vérifie le statut du service d'intégration « testservice » et s'il a été exécuté, il reçoit des détails pour la session « s_testSessionTask ».

```
#!/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
```

Entrée d'options de commande

pmcmd propose plusieurs manières d'entrer des options et des arguments de commande. Par exemple, pour entrer un mot de passe, utilisez la syntaxe suivante :

```
<<-password|-p> password<-passwordvar|-pv> passwordEnvVar>
```

Pour entrer un mot de passe, précédez le mot de passe de l'option -password ou -p :

```
-password ThePassword
or
-p ThePassword
```

Si vous utilisez une variable d'environnement de mot de passe, précédez le nom de variable de l'option `-pv` ou `-passwordvar` :

```
-passwordvar PASSWORD
or
-pv PASSWORD
```

Si une option de commande contient des espaces, utilisez des guillemets simples ou doubles pour entourer l'option. Par exemple, utilisez des guillemets simples dans la syntaxe suivante pour entourer le nom de dossier :

```
abortworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f 'quarterly sales' -
wait wf_MyWorkflow
```

Pour désigner une chaîne vide, utilisez deux guillemets simples (") ou deux guillemets doubles (").

aborttask

Abandonne une tâche. Exécutez cette commande seulement si le service d'intégration n'arrive pas à arrêter la tâche lorsque vous exécutez la commande `stoptask`.

La commande `pmcmd aborttask` utilise la syntaxe suivante en mode ligne de commande :

```
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
```

La commande `pmcmd aborttask` utilise la syntaxe suivante en mode interactif :

```
aborttask

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

[-wait|-nowait]

taskInstancePath
```


Le tableau suivant décrit les options et arguments de la commande `pmcmd aborttask` :

Option	Argument	Description
-service -sv	service	Requis en mode ligne de commande. Nom du service d'intégration. Pas utilisé en mode interactif.
-domain -d	domain	Facultatif en mode ligne de commande. Nom du domaine. Pas utilisé en mode interactif.
-timeout -t	timeout	Facultatif en mode ligne de commande. Durée, en secondes, pendant laquelle la commande <code>pmcmd</code> tente de se connecter au service d'intégration. Pas utilisé en mode interactif. Si l'option <code>-timeout</code> est omise, <code>pmcmd</code> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si la variable d'environnement n'est pas définie, <code>pmcmd</code> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.
-user -u	username	Requis en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de nom d'utilisateur. Nom d'utilisateur. Pas utilisé en mode interactif.
-uservar -uv	userEnvVar	Requis en mode ligne de commande si vous ne spécifiez pas le nom d'utilisateur. Spécifie la variable d'environnement de nom d'utilisateur. Pas utilisé en mode interactif.
-password -p	mot de passe	Requis en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de mot de passe. Mot de passe. Pas utilisé en mode interactif.
-passwordvar -pv	passwordEnvVar	Requis en mode ligne de commande si vous ne spécifiez pas le mot de passe. Variable d'environnement de mot de passe. Pas utilisé en mode interactif.
-usersecuritydomain -usd	usersecuritydomain	Facultatif en mode ligne de commande. Requis si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Pas utilisé en mode interactif. La valeur par défaut est Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Facultatif en mode ligne de commande. Variable d'environnement de domaine de sécurité. Pas utilisé en mode interactif.
-folder -f	folder	Requis si le nom de la tâche n'est pas unique dans le référentiel. Nom du dossier contenant la tâche.
-workflow -w	workflow	Requis. Nom du flux de travail.

Option	Argument	Description
-wait -nowait	-	Facultatif. Configure le mode attente : <ul style="list-style-type: none"> - wait. Vous ne pouvez entrer une nouvelle commande <i>pmcmd</i> que si le service d'intégration a terminé la commande précédente. - nowait. Vous pouvez entrer une nouvelle commande <i>pmcmd</i> une fois que le service d'intégration a reçu la commande précédente. La valeur par défaut est nowait.
-runinsname -rn	runInsName	Nom de l'instance d'exécution du flux de travail contenant la tâche que vous souhaitez arrêter. Utilisez cette option si vous exécutez des flux de travail simultanés.
-wfrunid	workflowRunId	Identifiant d'exécution (Run ID) de l'instance d'exécution du flux de travail qui contient la tâche que vous souhaitez abandonner. Utilisez cette option si vous exécutez des flux de travail simultanés. Remarque: Utilisez cette option si le flux de travail n'a pas un nom d'instance d'exécution unique.
-	taskInstancePath	Indique un nom de tâche et l'endroit où la tâche apparaît dans le flux de travail. Si la tâche se trouve dans un flux de travail, entrez le nom de la tâche uniquement. Si la tâche se trouve dans un worklet, entrez WorkletName.TaskName. Entrez taskInstancePath sous la forme d'une chaîne complète.

abortworkflow

Abandonne un flux de travail. Exécutez cette commande seulement si le service d'intégration n'arrive pas à arrêter le flux de travail en exécutant la commande stopworkflow.

La commande abortworkflow utilise la syntaxe suivante en mode ligne de commande :

```
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
```

La commande `abortworkflow` utilise la syntaxe suivante en mode interactif :

```
abortworkflow  
[<-folder|-f> folder]  
[-wait|-nowait]  
[<-runinsname|-rin> runInsName]  
[-wfrunid workflowRunId]  
workflow
```

Le tableau suivant décrit les options et arguments de `pmcmd abortworkflow` :

Option	Argument	Description
-service -sv	service	Obligatoire en mode ligne de commande. Nom du service d'intégration. Pas utilisé en mode interactif.
-domain -d	domaine	Facultatif en mode ligne de commande. Nom de domaine. Pas utilisé en mode interactif.
-timeout -t	timeout	Facultatif en mode ligne de commande. Durée en secondes pendant laquelle <i>pmcmd</i> tente de se connecter au service d'intégration. Pas utilisé en mode interactif. Si l'option -timeout est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.
-user -u	username	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de nom d'utilisateur. Nom d'utilisateur. Pas utilisé en mode interactif.
-uservar -uv	userEnvVar	Spécifie la variable d'environnement de nom d'utilisateur. Obligatoire en mode ligne de commande si vous ne spécifiez pas le nom d'utilisateur. Pas utilisé en mode interactif.
-password -p	password	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de mot de passe. Mot de passe. Pas utilisé en mode interactif.
-passwordvar -pv	passwordEnvVar	Obligatoire en mode ligne de commande si vous ne spécifiez pas le mot de passe. Variable d'environnement de mot de passe. Pas utilisé en mode interactif.
-usersecuritydomain -usd	usersecuritydomain	Facultatif en mode ligne de commande. Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Pas utilisé en mode interactif. La valeur par défaut est Natif.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Facultatif en mode ligne de commande. Variable d'environnement de domaine de sécurité. Pas utilisé en mode interactif.

Option	Argument	Description
-folder -f	dossier	Obligatoire si le nom de flux de travail n'est pas unique dans le référentiel. Nom du dossier contenant le flux de travail.
-wait -nowait	-	Facultatif. Configure le mode attente : <ul style="list-style-type: none"> - wait. Vous ne pouvez entrer une nouvelle commande <i>pmcmd</i> que si le service d'intégration a terminé la commande précédente. - nowait. Vous pouvez entrer une nouvelle commande <i>pmcmd</i> une fois que le service d'intégration a reçu la commande précédente. La valeur par défaut est nowait.
-runinsname -rin	runInsName	Nom de l'instance d'exécution du flux de travail que vous voulez arrêter. Utilisez cette option si vous exécutez des flux de travail simultanés.
-wfrunid	workflowRunId	Identifiant d'exécution (Run ID) de l'instance d'exécution du flux de travail que vous voulez arrêter. Utilisez cette option si vous exécutez des flux de travail simultanés. Remarque: Utilisez cette option si le flux de travail n'a pas un nom d'instance d'exécution unique.
-	flux de travail	Obligatoire. Nom du flux de travail.

Connect

Connecte le programme *pmcmd* au service d'intégration en mode interactif. Si vous omettez les informations de connexion, *pmcmd* vous invite à entrer les informations correctes. Une fois *pmcmd* correctement connecté, vous pouvez exécuter les commandes sans entrer à nouveau les informations de connexion.

```
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>]
```

Remarque: Utilisez cette commande uniquement en mode interactif de *pmcmd*.

Le tableau suivant décrit les options et arguments de *pmcmd* Connect :

Option	Argument	Description
-service -sv	service	Obligatoire. Nom du service d'intégration.
-domain -d	domaine	Facultatif. Nom de domaine.

Option	Argument	Description
-timeout -t	timeout	Facultatif. Durée en secondes pendant laquelle <i>pmcmd</i> tente de se connecter au service d'intégration. Si l'option -timeout est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. Par défaut 180.
-user -u	username	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de nom d'utilisateur. Nom d'utilisateur. Pas utilisé en mode interactif.
-uservar -uv	userEnvVar	Spécifie la variable d'environnement de nom d'utilisateur. Obligatoire en mode ligne de commande si vous ne spécifiez pas le nom d'utilisateur. Pas utilisé en mode interactif.
-password -p	mot de passe	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de mot de passe. Mot de passe. Pas utilisé en mode interactif.
-passwordvar -pv	passwordEnvVar	Obligatoire en mode ligne de commande si vous ne spécifiez pas le mot de passe. Variable d'environnement de mot de passe. Pas utilisé en mode interactif.
-usersecuritydomain -usd	usersecuritydomain	Facultatif en mode ligne de commande. Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Pas utilisé en mode interactif. La valeur par défaut est Natif.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Facultatif en mode ligne de commande. Variable d'environnement de domaine de sécurité. Pas utilisé en mode interactif.

Déconnecter

Déconnecte *pmcmd* du service d'intégration. Cela ne ferme pas le programme *pmcmd*. Utilisez cette commande lorsque vous voulez vous déconnecter d'un service d'intégration et vous connecter à un autre en mode interactif.

La commande Disconnect utilise la syntaxe suivante en mode interactif :

```
Disconnect
```

Remarque: Utilisez cette commande uniquement en mode interactif de *pmcmd*.

Exit

Déconnecte *pmcmd* du service d'intégration et ferme le programme *pmcmd*.

La commande Exit utilise la syntaxe suivante en mode interactif :

```
Exit
```

Remarque: Utilisez cette commande uniquement en mode interactif de *pmcmd*.

getrunningessionsdetails

Renvoie les détails suivants pour toutes les sessions en cours d'exécution sur un service d'intégration :

- Statut du service d'intégration, heure de démarrage et heure actuelle
- Nom de dossier et de flux de travail
- Instances de worklet et de session
- Pour chaque session d'exécution : type de tâche, heure de démarrage, statut d'exécution, premier code d'erreur, service d'intégration associé, mode d'exécution et nom de nœud
- Pour le mappage dans une session en cours d'exécution : nom de mappage, fichier journal de session, premier code d'erreur et message d'erreur, nombre de lignes source et cible ayant réussi et échoué et le nombre de messages d'erreur de transformation
- Nombre de sessions en cours d'exécution dans le service d'intégration

La commande *pmcmd* *getrunningessionsdetails* utilise la syntaxe suivante en mode ligne de commande :

```
pmcmd getrunningessionsdetails

<<-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>]
```

La commande *pmcmd* *getrunningessionsdetails* utilise la syntaxe suivante en mode interactif :

```
getrunningessionsdetails
```

Le tableau suivant décrit les options et arguments de la commande *pmcmd* *getrunningessionsdetails* :

Option	Argument	Description
-service -sv	service	Requis. Nom du service d'intégration.
-domain -d	domain	Facultatif. Nom du domaine.
-timeout -t	timeout	Facultatif. Durée, en secondes, pendant laquelle la commande <i>pmcmd</i> tente de se connecter au service d'intégration. Si l'option -timeout est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.

Option	Argument	Description
-user -u	username	Requis en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de nom d'utilisateur. Nom d'utilisateur. Pas utilisé en mode interactif.
-uservar -uv	userEnvVar	Spécifie la variable d'environnement de nom d'utilisateur. Requis en mode ligne de commande si vous ne spécifiez pas le nom d'utilisateur. Pas utilisé en mode interactif.
-password -p	mot de passe	Requis en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de mot de passe. Mot de passe. Pas utilisé en mode interactif.
-passwordvar -pv	passwordEnvVar	Requis en mode ligne de commande si vous ne spécifiez pas le mot de passe. Variable d'environnement de mot de passe. Pas utilisé en mode interactif.
-usersecuritydomain -usd	usersecuritydomain	Facultatif en mode ligne de commande. Requis si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Pas utilisé en mode interactif. La valeur par défaut est Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Facultatif en mode ligne de commande. Variable d'environnement de domaine de sécurité. Pas utilisé en mode interactif.

GetServiceDetails

Renvoie les détails suivants sur un service d'intégration :

- Nom du service d'intégration, statut, heure de démarrage et heure actuelle
- Pour chaque flux de travail actif : nom de dossier, nom de flux de travail, version, statut d'exécution, premier code d'erreur, heure de démarrage, fichier journal, type d'exécution, utilisateur exécutant le flux de travail
- Pour chaque tâche active : nom de dossier, nom et version de workflow, nom et version de l'instance de tâche, type de tâche, heure de début et de fin, statut d'exécution, premier code d'erreur, message d'erreur, service d'intégration associé, mode d'exécution, noms de nœuds sur lesquels les tâches sont exécutées
- Nombre de flux de travail et de sessions actifs et en attente

La commande GetServiceDetails utilise la syntaxe suivante en mode ligne de commande :

```
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]
```

La commande `GetServiceDetails` utilise la syntaxe suivante en mode interactif :

```
GetServiceDetails  
[  
  -all|-running|-scheduled  
]
```

Le tableau suivant décrit les options et arguments de `pmcmd GetServiceDetails` :

Option	Argument	Description
-service -sv	service	Obligatoire. Nom du service d'intégration.
-domain -d	domaine	Facultatif. Nom de domaine.
-timeout -t	timeout	Facultatif. Durée en secondes pendant laquelle <i>pmcmd</i> tente de se connecter au service d'intégration. Si l'option -timeout est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.
-user -u	username	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de nom d'utilisateur. Nom d'utilisateur. Pas utilisé en mode interactif.
-uservar -uv	userEnvVar	Spécifie la variable d'environnement de nom d'utilisateur. Obligatoire en mode ligne de commande si vous ne spécifiez pas le nom d'utilisateur. Pas utilisé en mode interactif.
-password -p	password	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de mot de passe. Mot de passe. Pas utilisé en mode interactif.
-passwordvar -pv	passwordEnvVar	Obligatoire en mode ligne de commande si vous ne spécifiez pas le mot de passe. Variable d'environnement de mot de passe. Pas utilisé en mode interactif.
-usersecuritydomain -usd	usersecuritydomain	Facultatif en mode ligne de commande. Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Pas utilisé en mode interactif. La valeur par défaut est Natif.

Option	Argument	Description
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Facultatif en mode ligne de commande. Variable d'environnement de domaine de sécurité. Pas utilisé en mode interactif.
-all -running -scheduled	-	Facultatif. Spécifie les flux de travail pour lesquels renvoyer des détails : <ul style="list-style-type: none"> - all. Renvoie les détails du statut des flux de travail en exécution et des flux de travail planifiés. - en exécution. Renvoie les détails du statut des flux de travail actifs. Les flux de travail actifs comprennent les flux de travail en exécution, en cours de suspension et suspendus. - programmé. Renvoie les détails du statut des flux de travail planifiés. La valeur par défaut est all.

getserviceproperties

Renvoie les informations suivantes sur le service d'intégration PowerCenter :

- Domaine dans lequel le service d'intégration PowerCenter s'exécute
- Nom et version du service d'intégration PowerCenter
- Si le service d'intégration PowerCenter autorise l'exécution de mappages de débogage
- Mode de mouvement de données
- Service de référentiel associé
- Heure de démarrage et horodatage actuel
- Nom de la grille
- Noms, nœuds et pages de code pour le processus de service d'intégration associé à PowerCenter
- Mode de fonctionnement pour le service d'intégration PowerCenter

La commande `pmcmd getserviceproperties` utilise la syntaxe suivante en mode ligne de commande :

```
pmcmd getserviceproperties
<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>
```

La commande `pmcmd getserviceproperties` utilise la syntaxe suivante en mode interactif :

```
getserviceproperties
```

Le tableau suivant décrit les options et arguments de la commande `pmcmd getserviceproperties` :

Option	Argument	Description
-service -sv	service	Requis. Nom du service d'intégration PowerCenter.
-domain -d	domain	Facultatif. Nom du domaine.
-timeout -t	timeout	Facultatif. Durée, en secondes, pendant laquelle <i>pmcmd</i> tente de se connecter au service d'intégration PowerCenter. Si l'option -timeout est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.

getsessionstatistics

Renvoie les détails et les statistiques de la session. La commande renvoie les informations suivantes :

- Nom de dossier, nom de flux de travail, worklet ou instance de session et nom de mappage
- Nom et emplacement de fichier journal de session
- Nombre de lignes source et cible ayant réussi et échoué
- Nombre d'erreurs de transformation
- Premier code d'erreur et message d'erreur
- Statut d'exécution de la tâche
- Nom du service d'intégration associé
- Noms de la grille et du nœud où la session est exécutée

La commande renvoie également les informations suivantes pour chaque partition :

- Nom de la partition
- Pour chaque transformation dans une partition : instance de transformation, nom de la transformation, nombre de lignes appliquées, affectées et rejetées, débit, dernier code d'erreur, heure de démarrage et heure de fin

La commande `getsessionstatistics` utilise la syntaxe suivante en mode ligne de commande :

```
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
```

La commande `getsessionstatistics` utilise la syntaxe suivante en mode interactif :

```
getsessionstatistics

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

<-workflow|-w> workflow

taskInstancePath
```

Le tableau suivant décrit les options et arguments de `pmcmd getsessionstatistics` :

Option	Argument	Description
-service -sv	service	Obligatoire. Nom du service d'intégration.
-domain -d	domaine	Facultatif. Nom de domaine.
-timeout -t	timeout	Facultatif. Durée en secondes pendant laquelle <i>pmcmd</i> tente de se connecter au service d'intégration. Si l'option -timeout est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.
-user -u	username	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de nom d'utilisateur. Nom d'utilisateur. Pas utilisé en mode interactif.
-uservar -uv	userEnvVar	Spécifie la variable d'environnement de nom d'utilisateur. Obligatoire en mode ligne de commande si vous ne spécifiez pas le nom d'utilisateur. Pas utilisé en mode interactif.
-password -p	password	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de mot de passe. Mot de passe. Pas utilisé en mode interactif.
-passwordvar -pv	passwordEnvVar	Obligatoire en mode ligne de commande si vous ne spécifiez pas le mot de passe. Variable d'environnement de mot de passe. Pas utilisé en mode interactif.
-usersecuritydomain -usd	usersecuritydomain	Obligatoire si vous utilisez une authentification LDAP. Facultatif en mode ligne de commande. Nom du domaine de sécurité auquel appartient l'utilisateur. Pas utilisé en mode interactif. La valeur par défaut est Natif.

Option	Argument	Description
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Facultatif en mode ligne de commande. Variable d'environnement de domaine de sécurité. Pas utilisé en mode interactif.
-folder -f	dossier	Obligatoire si le nom de la tâche n'est pas unique dans le référentiel. Nom du dossier contenant la tâche.
-runinsname -rn	runInsName	Nom de l'instance d'exécution du flux de travail qui contient la tâche. Utilisez cette option si vous exécutez des flux de travail simultanés.
-wfrunid	workflowRunId	Identifiant d'exécution (Run ID) de l'instance d'exécution du flux de travail qui contient la tâche. Utilisez cette option si vous exécutez des flux de travail simultanés. Remarque: Utilisez cette option si le flux de travail n'a pas un nom d'instance d'exécution unique.
-workflow -w	flux de travail	Obligatoire. Nom du flux de travail.
-	taskInstancePath	Obligatoire. Indique un nom de tâche et l'endroit où elle apparaît dans le flux de travail. Si la tâche est dans un flux de travail, entrez le nom de la tâche uniquement. Si la tâche est dans un worklet, entrez WorkletName.TaskName. Entrez taskInstancePath sous la forme d'une chaîne complète.

gettaskdetails

Renvoie les informations suivantes sur une tâche :

- Nom de dossier, nom de flux de travail, nom d'instance de la tâche et type de tâche
- Heure de démarrage et heure de fin de la dernière exécution
- Statut d'exécution de la tâche, premier code d'erreur et message d'erreur
- Noms de la grille et du nœud où la tâche est exécutée
- Nom du service d'intégration associé
- Mode d'exécution de la tâche

Si la tâche est une session, la commande renvoie également les détails suivants :

- Mappage et nom du fichier journal de session
- Premier code et message d'erreur
- Lignes source et cible ayant réussi et échoué
- Nombre d'erreurs de transformation

La commande `pmcmd gettaskdetails` utilise la syntaxe suivante en mode ligne de commande :

```
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

```

La commande `pmcmd gettaskdetails` utilise la syntaxe suivante en mode interactif :

```

gettaskdetails

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-runinsname|-rin> runInsName]

taskInstancePath

```

Le tableau suivant décrit les options et arguments de la commande `pmcmd gettaskdetails` :

Option	Argument	Description
-service -sv	service	Requis. Nom du service d'intégration.
-domain -d	domain	Facultatif. Nom du domaine.
-timeout -t	timeout	Facultatif. Durée, en secondes, pendant laquelle la commande <i>pmcmd</i> tente de se connecter au service d'intégration. Si l'option -timeout est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.
-user -u	username	Requis en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de nom d'utilisateur. Nom d'utilisateur. Pas utilisé en mode interactif.
-uservar -uv	userEnvVar	Spécifie la variable d'environnement de nom d'utilisateur. Requis en mode ligne de commande si vous ne spécifiez pas le nom d'utilisateur. Pas utilisé en mode interactif.
-password -p	mot de passe	Requis en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de mot de passe. Mot de passe. Pas utilisé en mode interactif.
-passwordvar -pv	passwordEnvVar	Requis en mode ligne de commande si vous ne spécifiez pas le mot de passe. Variable d'environnement de mot de passe. Pas utilisé en mode interactif.

Option	Argument	Description
-usersecuritydomain -usd	usersecuritydomain	Facultatif en mode ligne de commande. Requis si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Pas utilisé en mode interactif. La valeur par défaut est Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Facultatif en mode ligne de commande. Variable d'environnement de domaine de sécurité. Pas utilisé en mode interactif.
-folder -f	folder	Requis si le nom de la tâche n'est pas unique dans le référentiel. Nom du dossier contenant la tâche.
-workflow -w	workflow	Requis si le nom de la tâche n'est pas unique dans le référentiel. Nom du dossier contenant la tâche.
-runinsname -rn	runInsName	Nom de l'instance d'exécution du flux de travail qui contient la tâche. Utilisez cette option si vous exécutez des flux de travail simultanés.
-	taskInstancePath	Requis. Indique un nom de tâche et l'endroit où la tâche apparaît dans le flux de travail. Si la tâche se trouve dans un flux de travail, entrez le nom de la tâche uniquement. Si la tâche se trouve dans un worklet, entrez WorkletName.TaskName. Entrez taskInstancePath sous la forme d'une chaîne complète.

getworkflowdetails

Renvoie les informations suivantes au sujet d'un flux de travail :

- Nom de dossier et nom de flux de travail
- Statut d'exécution du flux de travail
- Premier code d'erreur et message d'erreur
- Heure de démarrage et heure de fin
- Nom du fichier journal
- Type d'exécution du flux de travail
- Nom de l'utilisateur qui a exécuté le flux de travail en dernier
- Nom du service d'intégration associé

La commande `getworkflowdetails` utilise la syntaxe suivante en mode ligne de commande :

```
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
```

La commande `getworkflowdetails` utilise la syntaxe suivante en mode interactif :

```
getworkflowdetails

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

Le tableau suivant décrit les options et arguments de la commande `pmcmd getworkflowdetails` :

Option	Argument	Description
-service -sv	service	Requis. Nom du service d'intégration.
-domain -d	domaine	Facultatif. Nom du domaine.
-timeout -t	timeout	Facultatif. Durée en secondes pendant laquelle la commande <i>pmcmd</i> tente de se connecter au service d'intégration. Si l'option -timeout est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.
-user -u	username	Requis en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de nom d'utilisateur. Nom d'utilisateur. Pas utilisé en mode interactif.
-uservar -uv	userEnvVar	Spécifie la variable d'environnement de nom d'utilisateur. Requis en mode ligne de commande si vous ne spécifiez pas le nom d'utilisateur. Pas utilisé en mode interactif.
-password -p	mot de passe	Requis en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de mot de passe. Mot de passe. Pas utilisé en mode interactif.
-passwordvar -pv	passwordEnvVar	Requis en mode ligne de commande si vous ne spécifiez pas le mot de passe. Variable d'environnement de mot de passe. Pas utilisé en mode interactif.
-usersecuritydomain -usd	usersecuritydomain	Facultatif en mode ligne de commande. Requis si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Pas utilisé en mode interactif. La valeur par défaut est Natif.

Option	Argument	Description
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Facultatif en mode ligne de commande. Variable d'environnement de domaine de sécurité. Pas utilisé en mode interactif.
-folder -f	dossier	Requis si le nom de flux de travail n'est pas unique dans le référentiel. Nom du dossier contenant le flux de travail.
-runinsname -rin	runInsName	Nom de l'instance d'exécution du flux de travail. Utilisez cette option si vous exécutez des flux de travail simultanés.
-wfrunid	workflowRunId	Numéro d'identificateur d'exécution (ID d'exécution) de l'instance d'exécution du flux de travail. Utilisez cette option si vous exécutez des flux de travail simultanés. Remarque: Utilisez cette option si le flux de travail n'a pas un nom d'instance d'exécution unique.
-	flux de travail	Nom du flux de travail.

Le tableau suivant décrit les différents statuts des flux de travail :

Nom de l'état	Description
Abandonné	Vous choisissez d'arrêter la tâche ou le flux de travail à partir du moniteur de flux de travail ou à l'aide de la commande <i>pmcmd</i> . Le service d'intégration arrête le processus DTM et abandonne la tâche. Vous pouvez récupérer un flux de travail qui a été arrêté si la restauration du flux de travail est activée.
Abandon	Le service d'intégration est en train d'arrêter le flux de travail.
Désactivé	Sélectionnez l'option Désactivé dans les propriétés du flux de travail. Le flux de travail désactivé ne sera pas exécuté par le service d'intégration tant que l'option Désactivé est active.
A échoué	Le service d'intégration a fait échouer le flux de travail, car il a rencontré des erreurs. Un flux de travail ayant échoué ne peut être récupéré.
Préparation à l'exécution	Le service d'intégration attend un verrou d'exécution pour le flux de travail.
Exécution	Le flux de travail est en cours d'exécution par le service d'intégration.
Programmé	Vous planifiez l'exécution du flux de travail à une date ultérieure. Le service d'intégration exécute le flux de travail pour la durée planifiée.
Arrêté	Vous choisissez d'arrêter le flux de travail ou la tâche depuis le moniteur de flux de travail ou via la commande <i>pmcmd</i> . Le service d'intégration arrête le traitement de la tâche et de toutes les autres tâches dans son chemin. Le service d'intégration continue l'exécution des tâches simultanées. Vous pouvez récupérer un flux de travail qui a été arrêté si la restauration du flux de travail est activée.
Arrêt	Le service d'intégration est en train d'arrêter le flux de travail.
Réussi.	Le service d'intégration a correctement terminé le flux de travail.

Nom de l'état	Description
Suspendu	Le service d'intégration suspend le flux de travail, car une tâche a échoué et aucune autre tâche n'est exécutée dans le flux de travail. Cet état est disponible lorsque vous sélectionnez l'option Suspension ou Erreur. Un flux de travail suspendu peut être récupéré.
Suspension	Une tâche échoue dans le flux de travail lorsque les autres tâches sont toujours en cours d'exécution. Le service d'intégration arrête l'exécution des tâches ayant échoué et continue d'exécuter les tâches dans d'autres chemins. Cet état est disponible lorsque vous sélectionnez l'option Suspension ou Erreur.
Terminé	Le service d'intégration se ferme inopinément lors de l'exécution de ce flux de travail ou de cette tâche. Vous pouvez récupérer un flux de travail qui a été arrêté si la restauration du flux de travail est activée.
Mise en arrêt	Le service d'intégration est en cours d'interruption du flux de travail ou de la tâche.
Statut inconnu	Cet état s'affiche dans les cas suivants : <ul style="list-style-type: none"> - Le service d'intégration ne peut pas déterminer le statut du flux de travail ou de la tâche. - Le service d'intégration ne répond pas à un ping effectué depuis le moniteur de flux de travail. - Le moniteur de flux de travail n'arrive pas à se connecter au service d'intégration dans le délai de dépassement de résilience.
Déprogrammé	Vous supprimez un flux de travail de la planification.
Attente	Le service d'intégration attend des ressources disponibles pour exécuter le flux de travail ou la tâche. Par exemple, vous pouvez définir sur 10 le nombre maximal de tâches Session et commande simultanées pour chaque processus du service d'intégration sur le nœud. Si le service d'intégration exécute déjà 10 sessions simultanées, tous les autres flux de travail et toutes les autres tâches se verront attribuer le statut Attente jusqu'à ce que le service d'intégration soit dans la possibilité d'exécuter d'autres tâches.

La commande `getworkflowdetails` affiche les détails du type d'exécution du dernier flux de travail. Le type d'exécution du flux de travail fait référence à la méthode utilisée pour démarrer le flux de travail.

Le tableau suivant décrit les différents types d'exécution du flux de travail avec la commande `getworkflowdetails` :

Types d'exécution du flux de travail	Description
Demande d'utilisateur	A démarré un flux de travail manuellement.
Planifier	Le flux de travail est exécuté à l'heure planifiée.

help

Renvoie la syntaxe de commande spécifiée. Si vous n'indiquez pas le nom de commande, `pmcmd` répertorie toutes les commandes et leur syntaxe.

La commande `pmcmd help` utilise la syntaxe suivante en mode ligne de commande :

```
pmcmd help [command]
```

La commande `pmcmd help` utilise la syntaxe suivante en mode interactif :

```
help [command]
```

Le tableau suivant décrit les options et arguments de la commande `pmcmd help` :

Option	Argument	Description
-	command	Facultatif. Nom de commande. Si vous n'indiquez pas le nom de commande, <i>pmcmd</i> répertorie toutes les commandes et leur syntaxe.

pingservice

Vérifie que le service d'intégration est en cours d'exécution.

La commande `pmcmd pingservice` utilise la syntaxe suivante en mode ligne de commande :

```
pmcmd pingservice  
  
<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>
```

La commande `pmcmd pingservice` utilise la syntaxe suivante en mode interactif :

```
pingservice
```

Le tableau suivant décrit les options et arguments de la commande `pmcmd pingservice` :

Option	Argument	Description
-service -sv	service	Requis. Nom du service d'intégration.
-domain -d	domain	Facultatif. Nom du domaine.
-timeout -t	timeout	Facultatif. Durée, en secondes, pendant laquelle la commande <i>pmcmd</i> tente de se connecter au service d'intégration. Si l'option <code>-timeout</code> est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.

recoverworkflow

Récupère les flux de travail suspendus. Pour récupérer un flux de travail, spécifiez le nom de dossier et le nom de flux de travail. Le Service d'intégration récupère le flux de travail de tous les worklets suspendus ou échoués et de toutes les tâches de commande, de courriel et de session suspendues ou échouées.

La commande `pmcmd recoverworkflow` utilise la syntaxe suivante en mode ligne de commande :

```
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
```

La commande `pmcmd recoverworkflow` utilise la syntaxe suivante en mode interactif :

```
recoverworkflow

[<-folder|-f> folder]

[<-paramfile> paramfile]

[<-localparamfile|-lpf> localparamfile]

[-wait|-nowait]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

Le tableau suivant décrit les options et arguments de la commande `pmcmd recoverworkflow` :

Option	Argument	Description
-service -sv	service	Requis. Nom du service d'intégration.
-domain -d	domain	Facultatif. Nom du domaine.

Option	Argument	Description
-timeout -t	timeout	Facultatif. Durée, en secondes, pendant laquelle la commande <i>pmcmd</i> tente de se connecter au service d'intégration. Si l'option -timeout est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.
-user -u	username	Requis en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de nom d'utilisateur. Nom d'utilisateur. Pas utilisé en mode interactif.
-uservar -uv	userEnvVar	Spécifie la variable d'environnement de nom d'utilisateur. Requis en mode ligne de commande si vous ne spécifiez pas le nom d'utilisateur. Pas utilisé en mode interactif.
-password -p	mot de passe	Requis en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de mot de passe. Mot de passe. Pas utilisé en mode interactif.
-passwordvar -pv	passwordEnvVar	Requis en mode ligne de commande si vous ne spécifiez pas le mot de passe. Variable d'environnement de mot de passe. Pas utilisé en mode interactif.
-usersecuritydomain -usd	usersecuritydomain	Facultatif en mode ligne de commande. Requis si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Pas utilisé en mode interactif. La valeur par défaut est Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Facultatif en mode ligne de commande. Variable d'environnement de domaine de sécurité. Pas utilisé en mode interactif.
-folder -f	folder	Requis si le nom de flux de travail n'est pas unique dans le référentiel. Nom du dossier contenant le flux de travail.
-paramfile	paramfile	Facultatif. Détermine quel fichier de paramètres utiliser lorsqu'une tâche ou un flux de travail s'exécute. Cela écrase le fichier de paramètres configuré pour le flux de travail ou la tâche.
-localparamfile -lpf	localparamfile	Facultatif. Spécifie le fichier de paramètres sur une machine locale utilisé par <i>pmcmd</i> au démarrage d'un flux de travail.
-wait -nowait	-	Facultatif. Configure le mode attente : - wait. Vous ne pouvez entrer une nouvelle commande <i>pmcmd</i> que si le service d'intégration a terminé la commande précédente. - nowait. Vous pouvez entrer une nouvelle commande <i>pmcmd</i> une fois que le service d'intégration a reçu la commande précédente. La valeur par défaut est nowait.

Option	Argument	Description
-runinsname -rin	runInsName	Nom de l'instance d'exécution du flux de travail que vous voulez récupérer. Utilisez cette option si vous exécutez des flux de travail simultanés.
-wfrunid	workflowRunId	Identifiant d'exécution (Run ID) de l'instance d'exécution du flux de travail que vous voulez récupérer. Utilisez cette option si vous exécutez des flux de travail simultanés. Remarque: Utilisez cette option si le flux de travail n'a pas un nom d'instance d'exécution unique.
-	workflow	Requis. Nom du flux de travail.

scheduleworkflow

Demande au service d'intégration de planifier un flux de travail. Utilisez cette commande pour renouveler la planification d'un flux de travail qui a été supprimé du calendrier.

La commande `pmcmd scheduleworkflow` utilise la syntaxe suivante en mode ligne de commande :

```
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
```

La commande `pmcmd scheduleworkflow` utilise la syntaxe suivante en mode interactif :

```
scheduleworkflow

[<-folder|-f> folder]

workflow
```

Le tableau suivant décrit les options et arguments de la commande `pmcmd scheduleworkflow` :

Option	Argument	Description
-service -sv	service	Requis. Nom du service d'intégration.
-domain -d	domain	Facultatif. Nom du domaine.

Option	Argument	Description
-timeout -t	timeout	Facultatif. Durée, en secondes, pendant laquelle la commande <i>pmcmd</i> tente de se connecter au service d'intégration. Si l'option -timeout est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.
-user -u	username	Requis en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de nom d'utilisateur. Nom d'utilisateur. Pas utilisé en mode interactif.
-uservar -uv	userEnvVar	Spécifie la variable d'environnement de nom d'utilisateur. Requis en mode ligne de commande si vous ne spécifiez pas le nom d'utilisateur. Pas utilisé en mode interactif.
-password -p	mot de passe	Requis en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de mot de passe. Mot de passe. Pas utilisé en mode interactif.
-passwordvar -pv	passwordEnvVar	Requis en mode ligne de commande si vous ne spécifiez pas le mot de passe. Variable d'environnement de mot de passe. Pas utilisé en mode interactif.
-usersecuritydomain -usd	usersecuritydomain	Facultatif en mode ligne de commande. Requis si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Pas utilisé en mode interactif. La valeur par défaut est Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Facultatif en mode ligne de commande. Variable d'environnement de domaine de sécurité. Pas utilisé en mode interactif.
-folder -f	folder	Requis si le nom de flux de travail n'est pas unique dans le référentiel. Nom du dossier contenant le flux de travail.
-	workflow	Requis. Nom du flux de travail.

SetFolder

Désigne le dossier par défaut dans lequel vous souhaitez exécuter toutes les commandes suivantes. Après l'exécution de cette commande, vous n'avez plus besoin d'entrer un nom de dossier pour les commandes de flux de travail, de tâche et de session. Si vous entrez un nom de dossier dans une commande après la commande SetFolder, le nom de dossier écrase le nom de dossier par défaut seulement pour cette commande.

La commande SetFolder utilise la syntaxe suivante en mode interactif :

```
SetFolder folder
```

Remarque: Utilisez cette commande uniquement en mode interactif de *pmcmd*.

Le tableau suivant décrit les options et arguments de la commande *pmcmd* SetFolder :

Option	Argument	Description
-	dossier	Obligatoire. Nom du dossier.

SetNoWait

Vous pouvez exécuter la commande *pmcmd* en mode wait ou nowait. En mode wait, *pmcmd* revient à l'invite de commande ou au shell une fois la commande terminée. Vous ne pouvez pas exécuter les commandes suivantes tant que la commande précédente n'est pas terminée. En mode nowait, *pmcmd* revient immédiatement à l'invite de commande ou au shell. Vous n'avez pas besoin d'attendre qu'une commande se termine pour exécuter la commande suivante.

La commande SetNoWait exécute *pmcmd* en mode nowait. Le mode nowait est le mode par défaut.

La commande SetNoWait utilise la syntaxe suivante en mode interactif :

```
SetNoWait
```

Lorsque vous définissez le mode nowait, utilisez l'invite de commande *pmcmd* une fois que le service d'intégration exécute la précédente commande.

Remarque: Utilisez cette commande uniquement en mode interactif de *pmcmd*.

SetWait

Vous pouvez exécuter la commande *pmcmd* en mode wait ou nowait. En mode wait, *pmcmd* revient à l'invite de commande ou au shell une fois la commande terminée. Vous ne pouvez pas exécuter les commandes suivantes tant que la commande précédente n'est pas terminée. En mode nowait, *pmcmd* revient immédiatement à l'invite de commande ou au shell. Vous n'avez pas besoin d'attendre qu'une commande se termine pour exécuter la commande suivante.

La commande SetWait exécute *pmcmd* en mode attente. L'invite de commande *pmcmd* est disponible une fois que le service d'intégration a terminé la commande précédente.

La commande SetWait utilise la syntaxe suivante en mode interactif :

```
SetWait
```

Remarque: Utilisez cette commande uniquement en mode interactif de *pmcmd*.

ShowSettings

Renvoie le nom du domaine, le service d'intégration et le référentiel auxquels *pmcmd* est connecté. Cela affiche le nom d'utilisateur, le mode attente et le dossier par défaut.

La commande ShowSettings utilise la syntaxe suivante en mode interactif :

```
ShowSettings
```

Remarque: Utilisez cette commande uniquement en mode interactif de *pmcmd*.

StartTask

Démarre une tâche.

La commande *StartTask* utilise la syntaxe suivante en mode ligne de commande :

```
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
```

La commande *StartTask* utilise la syntaxe suivante en mode interactif :

```
pmcmd StartTask

[<-folder|-f> folder]

<-workflow|-w> workflow

<-paramfile> paramfile]

[-wait|-nowait]

[<-recovery|-norecovery>]

[<-runinsname|-rin> runInsName]

taskInstancePath
```

Le tableau suivant décrit les options et arguments de *pmcmd StartTask* :

Option	Argument	Description
-service -sv	service	Obligatoire. Nom du service d'intégration.
-domain -d	domaine	Facultatif. Nom de domaine.

Option	Argument	Description
-timeout -t	timeout	Facultatif. Durée en secondes pendant laquelle <i>pmcmd</i> tente de se connecter au service d'intégration. Si l'option -timeout est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.
-user -u	username	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de nom d'utilisateur. Nom d'utilisateur. Pas utilisé en mode interactif.
-uservar -uv	userEnvVar	Spécifie la variable d'environnement de nom d'utilisateur. Obligatoire en mode ligne de commande si vous ne spécifiez pas le nom d'utilisateur. Pas utilisé en mode interactif.
-password -p	password	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de mot de passe. Mot de passe. Pas utilisé en mode interactif.
-passwordvar -pv	passwordEnvVar	Obligatoire en mode ligne de commande si vous ne spécifiez pas le mot de passe. Variable d'environnement de mot de passe. Pas utilisé en mode interactif.
-usersecuritydomain -usd	usersecuritydomain	Facultatif en mode ligne de commande. Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Pas utilisé en mode interactif. La valeur par défaut est Natif.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Facultatif en mode ligne de commande. Variable d'environnement de domaine de sécurité. Pas utilisé en mode interactif.
-folder -f	dossier	Obligatoire si le nom de flux de travail n'est pas unique dans le référentiel. Nom du dossier contenant le flux de travail.
-workflow -w	flux de travail	Obligatoire. Nom du flux de travail.
-paramfile	paramfile	Facultatif. Détermine quel fichier de paramètres utiliser lorsqu'une tâche ou un flux de travail s'exécute. Cela écrase le fichier de paramètres configuré pour le flux de travail ou la tâche.
-wait -nowait	-	Facultatif. Configure le mode attente : <ul style="list-style-type: none"> - wait. Vous ne pouvez entrer une nouvelle commande <i>pmcmd</i> que si le service d'intégration a terminé la commande précédente. - nowait. Vous pouvez entrer une nouvelle commande <i>pmcmd</i> une fois que le service d'intégration a reçu la commande précédente. La valeur par défaut est nowait.

Option	Argument	Description
-recovery -norecovery	-	<p>Facultatif. Si la tâche est une session, le service d'intégration exécute la session selon la stratégie de récupération configurée.</p> <ul style="list-style-type: none"> - récupération. Pour les sessions en temps réel pour lesquelles la récupération est activée, le service d'intégration récupère la session échouée et interrompt les autres tâches du flux de travail. <p>L'option de récupération est identique à l'option Recover Task dans le gestionnaire de flux de travail. Cette option n'est pas applicable pour les sessions dont la récupération n'est pas activée.</p> <ul style="list-style-type: none"> - norecovery. Pour les sessions en temps réel dont la récupération est activée, le service d'intégration ne traite pas les données de récupération. Le service d'intégration efface l'état de fonctionnement et le fichier ou la table de récupération avant de redémarrer la tâche. Pour les sessions dont la récupération n'est pas activée, le service d'intégration efface l'état de fonctionnement et redémarre la tâche. <p>L'option norecovery est identique à l'option Cold Start Task dans le gestionnaire de flux de travail.</p> <p>Si vous ne fournissez pas d'option pour les sessions dont la récupération est activée, le service d'intégration exécute la session en mode recovery. Si vous ne fournissez pas d'option pour les sessions dont la récupération n'est pas activée, le service d'intégration exécute la session en mode norecovery.</p>
-runinsname -rn	runInsName	Nom de l'instance d'exécution du flux de travail qui contient la tâche à démarrer. Utilisez cette option si vous exécutez des flux de travail simultanés.
-	taskInstancePath	Obligatoire. Indique un nom de tâche et l'endroit où elle apparaît dans le flux de travail. Si la tâche est dans un flux de travail, entrez le nom de la tâche uniquement. Si la tâche est dans un worklet, entrez WorkletName.TaskName. Entrez taskInstancePath sous la forme d'une chaîne complète.

Utilisation des fichiers de paramètres avec StartTask

Lorsque vous démarrez une tâche, vous pouvez éventuellement entrer le répertoire et le nom d'un fichier de paramètres. Le service d'intégration exécute la tâche avec les paramètres du fichier que vous indiquez.

Pour les utilisateurs du shell UNIX, placez le nom du fichier de paramètres entre guillemets simples :

```
-paramfile '$PMRootDir/myfile.txt'
```

Pour les utilisateurs de l'invite de commande Windows, le nom du fichier de paramètres ne peut pas avoir d'espaces au début ou à la fin. Si le nom comprend des espaces, placez le nom du fichier entre guillemets doubles :

```
-paramfile "$PMRootDir\my file.txt"
```

Quand vous écrivez une commande *pmcmd* qui inclut un fichier de paramètres situé sur une autre machine, utilisez la barre oblique inversée (\) avec le signe dollar (\$). Ceci garantit que la machine où la variable est définie développe la variable de processus.

```
pmcmd starttask -sv MyIntService -d MyDomain -uv USERNAME -pv PASSWORD -f east -w
wSalesAvg -paramfile '\\$PMRootDir/myfile.txt' taskA
```

StartWorkflow

Démarre un flux de travail.

La commande StartWorkflow utilise la syntaxe suivante en mode ligne de commande :

```
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
```

La commande StartWorkflow utilise la syntaxe suivante en mode interactif :

```
pmcmd StartWorkflow

[<-folder|-f> folder]

[<-startfrom> taskInstancePath [<-recovery|-norecovery>]]

[<-paramfile> paramfile]

[<-localparamfile|-lpf> localparamfile]

[<-osprofile|-o> osProfile]

[-wait|-nowait]

[<-runinsname|-rin> runInsName]

workflow
```

Le tableau suivant décrit les options et arguments de *pmcmd* StartWorkflow :

Option	Argument	Description
-service -sv	service	Obligatoire. Nom du service d'intégration.
-domain -d	domaine	Facultatif. Nom de domaine.

Option	Argument	Description
-timeout -t	timeout	Facultatif. Durée en secondes pendant laquelle <i>pmcmd</i> tente de se connecter au service d'intégration. Si l'option -timeout est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.
-user -u	username	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de nom d'utilisateur. Nom d'utilisateur. Pas utilisé en mode interactif.
-uservar -uv	userEnvVar	Spécifie la variable d'environnement de nom d'utilisateur. Obligatoire en mode ligne de commande si vous ne spécifiez pas le nom d'utilisateur. Pas utilisé en mode interactif.
-password -p	password	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de mot de passe. Mot de passe. Pas utilisé en mode interactif.
-passwordvar -pv	passwordEnvVar	Obligatoire en mode ligne de commande si vous ne spécifiez pas le mot de passe. Variable d'environnement de mot de passe. Pas utilisé en mode interactif.
-usersecuritydomain -usd	usersecuritydomain	Facultatif en mode ligne de commande. Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Pas utilisé en mode interactif. La valeur par défaut est Natif.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Facultatif en mode ligne de commande. Variable d'environnement de domaine de sécurité. Pas utilisé en mode interactif.
-folder -f	dossier	Obligatoire si le nom de flux de travail n'est pas unique dans le référentiel. Nom du dossier contenant le flux de travail.
-startfrom	taskInstancePath	Facultatif. Démarre un flux de travail depuis une tâche spécifiée, taskInstancePath. Si la tâche est dans un flux de travail, entrez le nom de la tâche uniquement. Si la tâche est dans un worklet, entrez WorkletName.TaskName. Entrez taskInstancePath sous la forme d'une chaîne complète. Si vous ne spécifiez pas un point de départ, le flux de travail démarre à la tâche de départ. Si la tâche est une session, spécifiez l'option -recovery ou -norecovery pour exécuter la session selon la stratégie de récupération configurée.
-paramfile	paramfile	Facultatif. Détermine quel fichier de paramètres utiliser lorsqu'une tâche ou un flux de travail s'exécute. Cela écrase le fichier de paramètres configuré pour le flux de travail ou la tâche.

Option	Argument	Description
-recovery -norecovery	-	<p>Facultatif. Le service d'intégration exécute la session selon la stratégie de récupération configurée.</p> <ul style="list-style-type: none"> - récupération. Pour les sessions en temps réel pour lesquelles la récupération est activée, le service d'intégration récupère la session échouée et interrompt les autres tâches du flux de travail. <p>L'option de récupération est identique à l'option Recover Workflow dans le gestionnaire de flux de travail. Cette option n'est pas applicable pour les sessions dont la récupération n'est pas activée.</p> <ul style="list-style-type: none"> - norecovery. Pour les sessions en temps réel dont la récupération est activée, le service d'intégration ne traite pas les données de récupération. Le service d'intégration efface l'état de fonctionnement et le fichier ou la table de récupération avant de redémarrer la tâche. Pour les sessions dont la récupération n'est pas activée, le service d'intégration efface l'état de fonctionnement et redémarre la tâche. <p>L'option norecovery est identique à l'option Cold Start Workflow dans le gestionnaire de flux de travail.</p> <p>Si vous ne fournissez pas d'option pour les sessions dont la récupération est activée, le service d'intégration exécute la session en mode recovery. Si vous ne fournissez pas d'option pour les sessions dont la récupération n'est pas activée, le service d'intégration exécute la session en mode norecovery.</p>
-localparamfile -lpf	localparamfile	Facultatif. Spécifie le fichier de paramètres sur une machine locale utilisé par <i>pmcmd</i> au démarrage d'un flux de travail.
-osprofile -o	osProfile	Facultatif. Spécifie le profil du système d'exploitation affecté au flux de travail.
-wait -nowait	-	<p>Facultatif. Configure le mode attente :</p> <ul style="list-style-type: none"> - wait. Vous ne pouvez entrer une nouvelle commande <i>pmcmd</i> que si le service d'intégration a terminé la commande précédente. - nowait. Vous pouvez entrer une nouvelle commande <i>pmcmd</i> une fois que le service d'intégration a reçu la commande précédente. <p>La valeur par défaut est nowait.</p>
-runinsname -rin	runInsName	Nom de l'instance d'exécution du flux de travail à démarrer. Utilisez cette option si vous exécutez des flux de travail simultanés.
-	flux de travail	Obligatoire. Nom du flux de travail.

Utilisation des fichiers de paramètres avec StartWorkflow

Lorsque vous démarrez un flux de travail, vous pouvez éventuellement entrer le répertoire et le nom d'un fichier de paramètres. Le service d'intégration exécute le flux de travail avec les paramètres du fichier que vous indiquez. Pour les utilisateurs du shell UNIX, placez le nom du fichier de paramètres entre guillemets simples. Pour les utilisateurs de l'invite de commande Windows, le nom du fichier de paramètres ne peut pas

avoir d'espaces au début ou à la fin. Si le nom comprend des espaces, placez le nom du fichier entre guillemets doubles.

Utilisez les fichiers de paramètres sur les machines suivantes :

- **Nœud exécutant le service d'intégration.** Quand vous utilisez un fichier de paramètres situé sur la machine du service d'intégration, utilisez l'option `-paramfile` pour indiquer l'emplacement et le nom du fichier de paramètres.

Sous UNIX, utilisez la syntaxe suivante :

```
-paramfile '$PMRootDir/myfile.txt'
```

Sous Windows, utilisez la syntaxe suivante :

```
-paramfile "$PMRootDir\my file.txt"
```

- **Machine locale.** Quand vous utilisez un fichier de paramètres dans lequel *pmcmd* est invoqué, *pmcmd* passe les valeurs et les variables du fichier au service d'intégration. Lorsque vous listez un fichier de paramètres local, spécifiez le chemin absolu ou relatif du fichier. Utilisez l'option `-localparamfile` ou `-lpf` pour indiquer l'emplacement et le nom du fichier de paramètres local.

Sous UNIX, utilisez la syntaxe suivante :

```
-lpf 'param_file.txt'
```

```
-lpf 'c:\Informatica\parameterfiles\param file.txt'
```

```
-localparamfile 'c:\Informatica\parameterfiles\param file.txt'
```

Sous Windows, utilisez la syntaxe suivante :

```
-lpf param_file.txt
```

```
-lpf "c:\Informatica\parameterfiles\param file.txt"
```

```
-localparamfile param_file.txt
```

- **Lecteurs réseau partagés.** Quand vous utilisez un fichier de paramètres situé sur une autre machine, utilisez la barre oblique inversée (`\`) avec le signe dollar (`$`). Ceci garantit que la machine où la variable est définie développe la variable de processus.

```
-paramfile '$PMRootDir/myfile.txt'
```

StopTask

Interrompt une tâche.

La commande `StopTask` utilise la syntaxe suivante en mode ligne de commande :

```
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
```

La commande **StopTask** utilise la syntaxe suivante en mode interactif :

```
pmcmd StopTask
[<-folder|-f> folder]
<-workflow|-w> workflow
[<-runinsname|-rin> runInsName]
[-wfrunid workflowRunId]
[-wait|-nowait]
taskInstancePath
```

Le tableau suivant décrit les options et arguments de *pmcmd StopTask* :

Option	Argument	Description
-service -sv	service	Obligatoire. Nom du service d'intégration.
-domain -d	domaine	Facultatif. Nom de domaine.
-timeout -t	timeout	Facultatif. Durée en secondes pendant laquelle <i>pmcmd</i> tente de se connecter au service d'intégration. Si l'option -timeout est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.
-user -u	username	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de nom d'utilisateur. Nom d'utilisateur. Pas utilisé en mode interactif.
-uservar -uv	userEnvVar	Spécifie la variable d'environnement de nom d'utilisateur. Obligatoire en mode ligne de commande si vous ne spécifiez pas le nom d'utilisateur. Pas utilisé en mode interactif.
-password -p	password	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de mot de passe. Mot de passe. Pas utilisé en mode interactif.
-passwordvar -pv	passwordEnvVar	Obligatoire en mode ligne de commande si vous ne spécifiez pas le mot de passe. Variable d'environnement de mot de passe. Pas utilisé en mode interactif.
-usersecuritydomain -usd	usersecuritydomain	Facultatif en mode ligne de commande. Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Pas utilisé en mode interactif. La valeur par défaut est Natif.

Option	Argument	Description
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Facultatif en mode ligne de commande. Variable d'environnement de domaine de sécurité. Pas utilisé en mode interactif.
-folder -f	dossier	Obligatoire si le nom de flux de travail n'est pas unique dans le référentiel. Nom du dossier contenant le flux de travail.
-workflow -w	flux de travail	Obligatoire. Nom du flux de travail.
-runinsname -rn	runInsName	Nom de l'instance d'exécution du flux de travail qui contient la tâche à arrêter. Utilisez cette option si vous exécutez des flux de travail simultanés.
-wfrunid	workflowRunId	Identifiant d'exécution (Run ID) de l'instance d'exécution du flux de travail qui contient la tâche à arrêter. Utilisez cette option si vous exécutez des flux de travail simultanés. Remarque: Utilisez cette option si le flux de travail n'a pas un nom d'instance d'exécution unique.
-wait -nowait	-	Facultatif. Configure le mode attente : - wait. Vous ne pouvez entrer une nouvelle commande <i>pmcmd</i> que si le service d'intégration a terminé la commande précédente. - nowait. Vous pouvez entrer une nouvelle commande <i>pmcmd</i> une fois que le service d'intégration a reçu la commande précédente. La valeur par défaut est nowait.
-	taskInstancePath	Obligatoire. Indique un nom de tâche et l'endroit où elle apparaît dans le flux de travail. Si la tâche est dans un flux de travail, entrez le nom de la tâche uniquement. Si la tâche est dans un worklet, entrez WorkletName.TaskName. Entrez taskInstancePath sous la forme d'une chaîne complète.

StopWorkflow

Arrête un flux de travail.

La commande StopWorkflow utilise la syntaxe suivante en mode ligne de commande :

```
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
```

La commande `StopWorkflow` utilise la syntaxe suivante en mode interactif :

```
pmcmd StopWorkflow
```

```
[<-folder|-f> folder]
```

```
[<-runinsname|-rin> runInsName]
```

```
[-wfrunid workflowRunId]
```

```
[-wait|-nowait]
```

```
workflow
```

Le tableau suivant décrit les options et arguments de `pmcmd StopWorkflow` :

Option	Argument	Description
-service -sv	service	Obligatoire. Nom du service d'intégration.
-domain -d	domaine	Facultatif. Nom de domaine.
-timeout -t	timeout	Facultatif. Durée en secondes pendant laquelle <i>pmcmd</i> tente de se connecter au service d'intégration. Si l'option -timeout est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.
-user -u	username	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de nom d'utilisateur. Nom d'utilisateur. Pas utilisé en mode interactif.
-uservar -uv	userEnvVar	Spécifie la variable d'environnement de nom d'utilisateur. Obligatoire en mode ligne de commande si vous ne spécifiez pas le nom d'utilisateur. Pas utilisé en mode interactif.
-password -p	password	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de mot de passe. Mot de passe. Pas utilisé en mode interactif.
-passwordvar -pv	passwordEnvVar	Obligatoire en mode ligne de commande si vous ne spécifiez pas le mot de passe. Variable d'environnement de mot de passe. Pas utilisé en mode interactif.
-usersecuritydomain -usd	usersecuritydomain	Facultatif en mode ligne de commande. Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Pas utilisé en mode interactif. La valeur par défaut est Natif.

Option	Argument	Description
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Facultatif en mode ligne de commande. Variable d'environnement de domaine de sécurité. Pas utilisé en mode interactif.
-folder -f	dossier	Obligatoire si le nom de flux de travail n'est pas unique dans le référentiel. Nom du dossier contenant le flux de travail.
-runinsname -rin	runInsName	Nom de l'instance d'exécution du flux de travail que vous voulez arrêter. Utilisez cette option si vous exécutez des flux de travail simultanés.
-wfrunid	workflowRunId	Identifiant d'exécution (Run ID) de l'instance d'exécution du flux de travail que vous voulez arrêter. Utilisez cette option si vous exécutez des flux de travail simultanés. Remarque: Utilisez cette option si le flux de travail n'a pas un nom d'instance d'exécution unique.
-wait -nowait	-	Facultatif. Configure le mode attente : - wait. Vous ne pouvez entrer une nouvelle commande <i>pmcmd</i> que si le service d'intégration a terminé la commande précédente. - nowait. Vous pouvez entrer une nouvelle commande <i>pmcmd</i> une fois que le service d'intégration a reçu la commande précédente. La valeur par défaut est nowait.
-	flux de travail	Obligatoire. Nom du flux de travail.

UnscheduleWorkflow

Retire un flux de travail d'un planificateur.

La commande `UnscheduleWorkflow` utilise la syntaxe suivante en mode ligne de commande :

```
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
```

La commande `UnscheduleWorkflow` utilise la syntaxe suivante en mode interactif :

```
UnscheduleWorkflow

[<-folder|-f> folder]

workflow
```

Le tableau suivant décrit les options et arguments de *pmcmd* *UnscheduleWorkflow* :

Option	Argument	Description
-service -sv	service	Obligatoire. Nom du service d'intégration.
-domain -d	domaine	Facultatif. Nom de domaine.
-timeout -t	timeout	Facultatif. Durée en secondes pendant laquelle <i>pmcmd</i> tente de se connecter au service d'intégration. Si l'option -timeout est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> . Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.
-user -u	username	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de nom d'utilisateur. Nom d'utilisateur. Pas utilisé en mode interactif.
-uservar -uv	userEnvVar	Spécifie la variable d'environnement de nom d'utilisateur. Obligatoire en mode ligne de commande si vous ne spécifiez pas le nom d'utilisateur. Pas utilisé en mode interactif.
-password -p	password	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de mot de passe. Mot de passe. Pas utilisé en mode interactif.
-passwordvar -pv	passwordEnvVar	Obligatoire en mode ligne de commande si vous ne spécifiez pas le mot de passe. Variable d'environnement de mot de passe. Pas utilisé en mode interactif.
-usersecuritydomain -usd	usersecuritydomain	Facultatif en mode ligne de commande. Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Pas utilisé en mode interactif. La valeur par défaut est Natif.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Facultatif en mode ligne de commande. Variable d'environnement de domaine de sécurité. Pas utilisé en mode interactif.
-folder -f	dossier	Obligatoire si le nom de flux de travail n'est pas unique dans le référentiel. Nom du dossier contenant le flux de travail.
-	flux de travail	Obligatoire. Nom du flux de travail.

UnsetFolder

Supprime la désignation d'un dossier par défaut. Après l'exécution de cette commande, vous devez spécifier un nom de dossier à chaque fois que vous entrez une commande pour une session, un flux de travail ou une tâche.

La commande `UnsetFolder` utilise la syntaxe suivante en mode interactif :

```
UnsetFolder
```

Remarque: Utilisez cette commande uniquement en mode interactif de *pmcmd*.

Version

Affiche la version de PowerCenter et les informations sur la marque commerciale et le copyright d'Informatica.

La commande `Version` utilise la syntaxe suivante en mode ligne de commande :

```
pmcmd Version
```

La commande `Version` utilise la syntaxe suivante en mode interactif :

```
Version
```

WaitTask

Demande au service d'intégration de terminer la tâche avant de renvoyer l'invite *pmcmd* à l'invite de commande ou au shell.

La commande `WaitTask` utilise la syntaxe suivante en mode ligne de commande :

```
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
```

La commande `WaitTask` utilise la syntaxe suivante en mode interactif :

```
WaitTask

[<-folder|-f> folder]

[<-workflow|-w> workflow]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

taskInstancePath
```

Le tableau suivant décrit les options et arguments de *pmcmd* WaitTask :

Option	Argument	Description
-service -sv	service	Obligatoire. Nom du service d'intégration.
-domain -d	domaine	Facultatif. Nom de domaine.
-timeout -t	timeout	Facultatif. Durée en secondes pendant laquelle <i>pmcmd</i> tente de se connecter au service d'intégration. Si l'option -timeout est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.
-user -u	username	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de nom d'utilisateur. Nom d'utilisateur. Pas utilisé en mode interactif.
-uservar -uv	userEnvVar	Spécifie la variable d'environnement de nom d'utilisateur. Obligatoire en mode ligne de commande si vous ne spécifiez pas le nom d'utilisateur. Pas utilisé en mode interactif.
-password -p	password	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de mot de passe. Mot de passe. Pas utilisé en mode interactif.
-passwordvar -pv	passwordEnvVar	Obligatoire en mode ligne de commande si vous ne spécifiez pas le mot de passe. Variable d'environnement de mot de passe. Pas utilisé en mode interactif.
-usersecuritydomain -usd	usersecuritydomain	Facultatif en mode ligne de commande. Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Pas utilisé en mode interactif. La valeur par défaut est Natif.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Facultatif en mode ligne de commande. Variable d'environnement de domaine de sécurité. Pas utilisé en mode interactif.
-folder -f	dossier	Obligatoire si le nom de la tâche n'est pas unique dans le référentiel. Nom du dossier contenant la tâche.
-workflow -w	flux de travail	Obligatoire. Nom du flux de travail.
-runinsname -rn	runInsName	Nom de l'instance d'exécution du flux de travail qui contient la tâche. Utilisez cette option si vous exécutez des flux de travail simultanés.

Option	Argument	Description
-wfrunid	workflowRunId	Identifiant d'exécution (Run ID) de l'instance d'exécution du flux de travail qui contient la tâche. Utilisez cette option si vous exécutez des flux de travail simultanés. Remarque: Utilisez cette option si le flux de travail n'a pas un nom d'instance d'exécution unique.
-	taskInstancePath	Obligatoire. Indique un nom de tâche et l'endroit où elle apparaît dans le flux de travail. Si la tâche est dans un flux de travail, entrez le nom de la tâche uniquement. Si la tâche est dans un worklet, entrez WorkletName.TaskName. Entrez taskInstancePath sous la forme d'une chaîne complète.

WaitWorkflow

Conduit *pmcmd* à attendre la terminaison d'un flux de travail pour exécuter les commandes suivantes. Utilisez cette commande en conjonction avec le code de retour quand vous exécutez *pmcmd* depuis un script. Par exemple, vous souhaitez peut-être vérifier l'état d'un flux de travail critique avant de démarrer un autre flux de travail. Utilisez la commande *WaitWorkflow* pour attendre la terminaison du flux de travail critique et vérifiez ensuite le code de retour de *pmcmd*. Si le code de retour est 0 (réussi), démarrez le flux de travail suivant.

La commande *WaitWorkflow* renvoie l'invite quand un flux de travail se termine.

La commande *WaitWorkflow* utilise la syntaxe suivante en mode ligne de commande :

```
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
```

La commande *WaitWorkflow* utilise la syntaxe suivante en mode interactif :

```
WaitWorkflow

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

Le tableau suivant décrit les options et arguments de *pmcmd* WaitWorkflow :

Option	Argument	Description
-service -sv	service	Obligatoire. Nom du service d'intégration.
-domain -d	domaine	Facultatif. Nom de domaine.
-timeout -t	timeout	Facultatif. Durée en secondes pendant laquelle <i>pmcmd</i> tente de se connecter au service d'intégration. Si l'option -timeout est omise, <i>pmcmd</i> utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si la variable d'environnement n'est pas définie, <i>pmcmd</i> utilise la valeur de dépassement de délai par défaut. La valeur par défaut est 180.
-user -u	username	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de nom d'utilisateur. Nom d'utilisateur. Pas utilisé en mode interactif.
-uservar -uv	userEnvVar	Spécifie la variable d'environnement de nom d'utilisateur. Obligatoire en mode ligne de commande si vous ne spécifiez pas le nom d'utilisateur. Pas utilisé en mode interactif.
-password -p	password	Obligatoire en mode ligne de commande si vous ne spécifiez pas la variable d'environnement de mot de passe. Mot de passe. Pas utilisé en mode interactif.
-passwordvar -pv	passwordEnvVar	Obligatoire en mode ligne de commande si vous ne spécifiez pas le mot de passe. Variable d'environnement de mot de passe. Pas utilisé en mode interactif.
-usersecuritydomain -usd	usersecuritydomain	Facultatif en mode ligne de commande. Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. Pas utilisé en mode interactif. La valeur par défaut est Natif.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Facultatif en mode ligne de commande. Variable d'environnement de domaine de sécurité. Pas utilisé en mode interactif.
-folder -f	dossier	Obligatoire si le nom de flux de travail n'est pas unique dans le référentiel. Nom du dossier contenant le flux de travail.
-runinsname -rin	runInsName	Nom de l'instance d'exécution du flux de travail. Utilisez cette option si vous exécutez des flux de travail simultanés.
-wfrunid	workflowRunId	Identifiant d'exécution (Run ID) de l'instance d'exécution du flux de travail. Utilisez cette option si vous exécutez des flux de travail simultanés. Remarque: Utilisez cette option si le flux de travail n'a pas un nom d'instance d'exécution unique.
-	flux de travail	Obligatoire. Nom du flux de travail.

CHAPITRE 44

Référence de commande pmrep

Ce chapitre comprend les rubriques suivantes :

- [Utilisation de pmrep, 1382](#)
- [AddToDeploymentGroup, 1387](#)
- [ApplyLabel, 1389](#)
- [AssignIntegrationService, 1391](#)
- [AssignPermission, 1392](#)
- [BackUp, 1393](#)
- [ChangeOwner, 1394](#)
- [CheckIn, 1395](#)
- [CleanUp, 1396](#)
- [ClearDeploymentGroup, 1396](#)
- [Connect, 1397](#)
- [Créer, 1399](#)
- [CreateConnection, 1400](#)
- [CreateDeploymentGroup, 1403](#)
- [CreateFolder, 1404](#)
- [CreateLabel, 1406](#)
- [CreateQuery, 1406](#)
- [Supprimer, 1412](#)
- [DeleteConnection, 1413](#)
- [DeleteDeploymentGroup, 1414](#)
- [DeleteFolder, 1414](#)
- [DeleteLabel, 1414](#)
- [DeleteObject , 1415](#)
- [DeleteQuery, 1416](#)
- [DeployDeploymentGroup, 1416](#)
- [DeployFolder, 1418](#)
- [ExecuteQuery, 1419](#)
- [Exit, 1421](#)
- [FindCheckout, 1421](#)
- [GetConnectionDetails, 1423](#)

- [GenerateAbapProgramToFile, 1423](#)
- [Aide, 1425](#)
- [InstallAbapProgram, 1425](#)
- [KillUserConnection, 1427](#)
- [ListConnections, 1428](#)
- [ListObjectDependencies , 1428](#)
- [ListObjects, 1431](#)
- [ListTablesBySess, 1436](#)
- [ListUserConnections, 1437](#)
- [MassUpdate, 1438](#)
- [ModifyFolder, 1444](#)
- [Notification, 1446](#)
- [ObjectExport, 1446](#)
- [ObjectImport , 1448](#)
- [PurgeVersion, 1449](#)
- [Enregistrement, 1451](#)
- [RegisterPlugin, 1453](#)
- [Restaurer, 1455](#)
- [RollbackDeployment , 1456](#)
- [Exécuter, 1457](#)
- [ShowConnectionInfo, 1458](#)
- [SwitchConnection, 1459](#)
- [TruncateLog, 1459](#)
- [UndoCheckout, 1460](#)
- [Désinscrire, 1461](#)
- [UnregisterPlugin, 1462](#)
- [UpdateConnection, 1464](#)
- [UpdateEmailAddr, 1466](#)
- [UpdateSeqGenVals, 1467](#)
- [UpdateSrcPrefix, 1468](#)
- [UpdateStatistics , 1469](#)
- [UpdateTargPrefix, 1470](#)
- [Mise à niveau, 1471](#)
- [UninstallAbapProgram, 1471](#)
- [Valider, 1473](#)
- [Version, 1475](#)

Utilisation de pmrep

pmrep est un programme de ligne de commande à utiliser pour mettre à jour les informations du référentiel et exécuter les fonctions du référentiel. *pmrep* est installé dans le Client Informatica et les répertoires bin des services PowerCenter.

Utilisez *pmrep* pour exécuter des tâches d'administration du référentiel telles que lister les objets du référentiel, créer et éditer des groupes, restaurer et supprimer des référentiels et mettre à jour les paramètres relatifs à la session ainsi que les informations de sécurité dans le référentiel PowerCenter.

Quand vous utilisez *pmrep*, vous pouvez entrer des commandes dans les modes suivants :

- **Mode ligne de commande.** Vous pouvez exécuter des commandes *pmrep* directement depuis la ligne de commande système. Utilisez le mode ligne de commande pour réaliser le script des commandes *pmrep*.
- **Mode interactif.** Vous pouvez exécuter les commandes *pmrep* depuis une invite interactive. *pmrep* ne se ferme pas après l'exécution de la commande.

Vous pouvez utiliser des variables d'environnement pour définir les noms d'utilisateur et les mots de passe pour *pmrep*. Avant d'utiliser *pmrep*, configurez ces variables. Les variables d'environnement s'appliquent aux commandes *pmrep* qui s'exécutent sur le nœud.

Toutes les commandes *pmrep* requièrent une connexion au référentiel, sauf les commandes suivantes :

- Aide
- ListAllPrivileges

Utilisez la commande *pmrep* Connect pour vous connecter au référentiel avant d'utiliser d'autres commandes *pmrep*.

Remarque: Si le domaine est un domaine multiversions, exécutez *pmrep* depuis le répertoire d'installation de la version du service de référentiel.

Exécution de commandes en mode ligne de commande

Le mode ligne de commande appelle et quitte *pmrep* chaque fois que vous exécutez une commande. Le mode ligne de commande est utile si vous souhaitez exécuter des commandes *pmrep* via des fichiers de lots, des scripts ou d'autres programmes.

Pour exécuter des commandes *pmrep* en mode ligne de commande :

1. À l'invite de commande, passez au répertoire abritant l'exécutable *pmrep*.
2. Entrez *pmrep* suivi du nom de commande et de ses options et arguments :

```
pmrep command_name [-option1] argument_1 [-option2] argument_2...
```

Exécution de commandes en mode interactif

Le mode interactif appelle *pmrep*. Vous pouvez émettre une série de commandes depuis une invite *pmrep* sans devoir quitter après chaque commande.

Pour exécuter des commandes *pmrep* en mode interactif :

1. À l'invite de commande, entrez *pmrep* pour appeler le mode interactif.
Ceci démarre *pmrep* en mode interactif et affiche l'invite *pmrep >*. Vous ne devez pas saisir *pmrep* avant chaque commande en mode interactif.
2. Entrez une commande et ses options et arguments.

À l'invite, entrez :

```
command_name [-option1] argument_1 [-option2] argument_2...
```

pmrep exécute la commande et affiche l'invite à nouveau.

3. Saisissez `exit` pour terminer la session interactive.

Exécution de commandes en mode normal et mode exclusif

Le service de référentiel s'exécute en mode normal ou en mode exclusif. Exécutez le service de référentiel en mode exclusif pour effectuer les tâches qui ne permettent qu'une seule connexion utilisateur au référentiel.

Exécutez le service de référentiel en mode exclusif pour utiliser les commandes *pmrep* suivantes :

- Créer
- Supprimer
- Enregistrement
- RegisterPlugin
- Désinscrire
- UnregisterPlugin

Vous pouvez utiliser l'outil Administrator ou *infacmd* pour exécuter le service de référentiel en mode exclusif.

Codes de retour pmrep

pmrep indique la réussite ou l'échec d'une commande à l'aide d'un code de retour. Le code de retour « 0 » indique que la commande a réussi. Code de retour « 1 » indique que la commande a échoué. Certaines des commandes effectuent plusieurs opérations. Par exemple, `AddToDeploymentgroup` ajoute plusieurs objets à un groupe de déploiement. Dans ce cas, un code de retour « 0 » indique que la commande a été correctement exécutée même si seuls certains des objets ont été correctement déployés.

Entrez l'une des commandes « echo » DOS ou UNIX suivantes immédiatement après avoir exécuté la commande *pmrep* :

- Dans un shell DOS, entrez `echo %ERRORLEVEL%`
- Dans un shell UNIX Bourne ou Korn, entrez `echo $?`
- Dans un shell C UNIX, entrez `echo $status`

Utilisation des chaînes de connexion natives

Certaines commandes *pmrep* telles que `CreateConnection` et `Restore`, requièrent une chaîne de connexion native.

Le tableau ci-dessous décrit la syntaxe de la chaîne de connexion native pour chaque référentiel de base de données pris en charge :

Base de données	Syntaxe de chaîne de connexion	Exemple
IBM DB2	<i>dbname</i>	mydatabase
Microsoft SQL Server	<i>servername@dbname</i>	sqlserver@mydatabase

Base de données	Syntaxe de chaîne de connexion	Exemple
Oracle	<i>dbname.world</i> (identique à l'entrée TNSNAMES)	oracle.world
Sybase ASE	servername@dbname	sambrown@mydatabase

Création de scripts de commandes pmrep

Lorsque vous utilisez la commande *pmrep*, vous pouvez utiliser régulièrement des commandes avec des options et des arguments spécifiques. Par exemple, vous pouvez utiliser *pmrep* pour effectuer une sauvegarde quotidienne d'un référentiel de production. Dans ce cas, vous pouvez créer un fichier de script qui appelle une ou plusieurs commandes *pmrep*, y compris leurs options et arguments.

Par exemple, le fichier de lots Windows suivant, *backupproduction.bat*, se connecte à et sauvegarde un référentiel appelé Production :

```
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
```

Vous pouvez exécuter des fichiers de script depuis l'interface de commande. Vous ne pouvez pas exécuter les fichiers de lot *pmrep* en mode interactif.

Conseils pour la création de scripts de commandes pmrep

Suivez les conseils suivants quand vous créez et exécutez des scripts *pmrep* :

- Incluez une commande Connect comme première commande appelée par le fichier de script. Ceci permet de vous assurer que vous effectuez les tâches sur le bon référentiel.
- Pour exécuter des scripts *pmrep* qui se connectent simultanément à différents référentiels, définissez la variable d'environnement INFA_REPCNX_INFO dans chaque environnement pour stocker le nom et le chemin du fichier de la connexion du référentiel. Cela empêche un script d'écraser les informations de connexion utilisée par un autre script.

Sous-types de connexion

Lorsque vous répertoriez ou mettez à jour une connexion, vous pouvez spécifier les sous-types de connexion en fonction du type de connexion associé. En fonction des plug-ins du référentiel, la commande *pmrep* répertorie les sous-types de connexion dans le référentiel, par défaut.

Le tableau suivant présente la liste des sous-types de connexion du type de connexion associé :

Type de connexion	Sous-type de connexion
Relationnel	Sybase
Relationnel	Informix (obsolète)
Relationnel	Microsoft SQL Server

Type de connexion	Sous-type de connexion
Relationnel	DB2
Relationnel	ODBC
Relationnel	Teradata
Relationnel	Netezza
Relationnel	Vertica
Relationnel	PowerChannel pour DB2
Relationnel	PowerChannel pour Oracle
Relationnel	PowerChannel pour MS SQL Server
Relationnel	PowerChannel pour ODBC
Relationnel	PWX DB2zOS
Relationnel	PWX DB2i5OS
Relationnel	PWX DB2LUW
Relationnel	PWX Oracle
Relationnel	PWX MSSQLServer
Relationnel	PWX NRDB Lookup
Relationnel	Teradata PT Connection
Application	SAP BW
Application	SAP R3
Application	PeopleSoft Oracle
Application	PeopleSoft Sybase
Application	PeopleSoft Informix
Application	PeopleSoft MsSqlserver
Application	PeopleSoft Db2
Application	Siebel Oracle
Application	Siebel Sybase
Application	Siebel Informix
Application	Siebel MsSqlserver

Type de connexion	Sous-type de connexion
Application	Siebel Db2
Application	SAP_ALE_IDoc_Reader
Application	SAP Type A
Application	SAP_BWOHS_READER
Application	SAP_ALE_IDoc_Writer
Application	Interface SAP RFC/BAPI
Application	Connexion JNDI
Application	Connexion JMS
Application	webMethods Broker
Application	Serveur d'intégration webMethods
Application	Consommateur de services Web
Application	PWX NRDB Batch
Application	PWX NRDB CDC Change
Application	PWX NRDB CDC Real Time
Application	PWX DB2zOS CDC Change
Application	PWX DB2zOS CDC Real Time
Application	PWX DB2i5OS CDC Change
Application	PWX DB2i5OS CDC Real Time
Application	HTTP Transformation
Application	PWX Oracle CDC Change
Application	PWX Oracle CDC Real Time
Application	LMAPITarget
Application	Connexion Teradata FastExport
Application	PWX MSSQL CDC Change
Application	PWX MSSQL CDC Real Time
Application	PWX DB2LUW CDC Change
Application	PWX DB2LUW CDC Real Time

Type de connexion	Sous-type de connexion
Application	Connexion Salesforce
Application	Connexion HDFS Hadoop
FTP	FTP
Chargeur externe	Chargeur externe Teradata Mload
Chargeur externe	Chargeur externe Teradata Tump
Chargeur externe	Chargeur externe DB2 EE
Chargeur externe	Chargeur externe DB2 EEE
Chargeur externe	Chargeur externe Teradata FastLoad
Chargeur externe	Chargeur externe Teradata Warehouse Builder
Chargeur externe	HP NeoView Java Transporter
File d'attente	File d'attente de messages
File d'attente	MSMQ

AddToDeploymentGroup

Ajoute des objets à un groupe de déploiement. Utilisez AddToDeploymentGroup pour ajouter une source, une cible, une transformation, un mappage, une session, un worklet, un flux de travail, un planificateur, une configuration de session et des tâches d'objets.

Vous ne pouvez pas ajouter des objets extraits à un groupe de déploiement. Vous pouvez spécifier des objets en utilisant les options de commande ou un fichier d'entrée persistant. Si vous utilisez un fichier d'entrée persistant, vous pouvez entrer l'option nom du groupe de déploiement.

Utilisez AddToDeploymentGroup pour ajouter les objets d'entrée réutilisables. Si vous voulez ajouter des objets d'entrée non réutilisables, vous devez utiliser un fichier d'entrée persistant contenant les identifiants des objets encodés.

Si la commande AddToDeploymentGroup fonctionne correctement, soit elle ne renvoie aucune information, soit elle renvoie une liste des objets déjà présents dans le groupe de déploiement. Si la commande échoue, la raison de l'échec est affichée.

La commande AddToDeploymentGroup utilise la syntaxe suivante :

```
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]

```

Le tableau suivant décrit les options et arguments de la commande *pmrep AddToDeploymentGroup* :

Option	Argument	Description
-p	deployment_group_name	Obligatoire. Nom du groupe de déploiement auquel ajouter des objets.
-n	object_name	Obligatoire lorsque vous ajoutez un objet spécifique. Nom de l'objet que vous ajoutez au groupe de déploiement. Vous ne pouvez pas entrer le nom d'un objet extrait. Vous ne pouvez pas utiliser l'option -n si vous utilisez l'option -i.
-o	object_type	Obligatoire lors de l'ajout d'un objet spécifique. Type d'objet que vous ajoutez. Vous pouvez spécifier la source, la cible, la transformation, le mappage, la session, le worklet, le flux de travail, le planificateur, la configuration de session, la tâche, le cube et la dimension.
-t	object_subtype	Obligatoire lorsque vous utilisez des sous-types valides. Type de tâche ou de transformation que vous ajoutez. Pour plus d'informations sur les sous-types valides, consultez "Liste des types d'objets" à la page 1433 .
-v	version_number	Facultatif. Version de l'objet à ajouter. La valeur par défaut est la dernière version de l'objet. La commande échoue si vous spécifiez un numéro de version pour un référentiel sans version.
-f	folder_name	Obligatoire lorsque vous entrez un nom d'objet. Dossier qui contient l'objet que vous ajoutez.
-i	persistent_input_file	Fichier texte généré à partir de executeQuery, Validate ou ListObjectDependencies contenant une liste des enregistrements d'objets avec des identifiants encodés. Si vous utilisez ce paramètre, <i>pmrep</i> n'autorise pas les options -n, -o et -f.

Option	Argument	Description
-d	dependency_types	<p>Facultatif. Objets dépendants à ajouter au groupe de déploiement avec l'objet. Entrez l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> - all. <i>pmrep</i> ajoute les objets et tous les objets dépendants, réutilisables ou non réutilisables, au groupe de déploiement. - « non réutilisables ». <i>pmrep</i> ajoute les objets et les objets dépendants non réutilisables correspondants, au groupe de déploiement. - aucun. <i>pmrep</i> n'ajoute pas d'objets dépendants au groupe de déploiement. <p>Si vous omettez ce paramètre, <i>pmrep</i> ajoute les objets et tous les objets dépendants au groupe de déploiement.</p> <p>Remarque: Mettez les arguments qui contiennent des espaces ou des caractères non alphanumériques entre guillemets.</p>
-s	dbd_separator	<p>Facultatif. Si une source ODBC comporte un point (.) dans le nom, définissez un autre caractère de séparation lorsque vous définissez l'objet source. Par exemple, au lieu de database_name.source_name, définissez l'objet source comme database_name\source_name et définissez dbd_separator comme une barre oblique inversée (\).</p>

ApplyLabel

Applique un libellé à un objet ou à un ensemble d'objets dans un dossier. Si vous entrez un nom de dossier, tous les objets du dossier reçoivent le libellé. Vous pouvez appliquer le libellé aux objets dépendants. Si vous utilisez l'option *dependency_object_types*, *pmrep* donne un libellé à tous les objets dépendants. Pour appliquer un libellé aux objets dépendants sélectionnés, séparez chaque nom de type d'objet par une virgule sans espace entre eux dans la ligne de commande.

Utilisez ApplyLabel pour mettre un libellé aux objets d'entrée réutilisables. Si vous voulez mettre un libellé aux objets d'entrée non réutilisables, vous devez utiliser un fichier d'entrée persistant contenant les identifiants des objets encodés.

Si ApplyLabel réussit, soit *pmrep* n'affiche aucune information de statut, soit la commande affiche une liste d'objets qui ont déjà le libellé. Si la commande échoue, *pmrep* affiche la raison de l'échec.

La commande ApplyLabel utilise la syntaxe suivante :

```
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]

```

Le tableau suivant décrit les options et arguments de *pmrep* ApplyLabel :

Option	Argument	Description
-a	label_name	Obligatoire. Nom du libellé à appliquer à l'objet.
-n	object_name	Obligatoire si vous êtes en train de mettre à jour un objet spécifique. Nom de l'objet destiné à recevoir le libellé. Vous ne pouvez pas entrer les noms d'objet si vous utilisez l'option -i.
-o	object_type	Type d'objet auquel appliquer le libellé. Vous pouvez spécifier la source, la cible, la transformation, le mappage, la session, le worklet, le flux de travail, le planificateur, la configuration de session, la tâche, le cube ou la dimension. Obligatoire lors de l'application d'un libellé à un objet spécifique.
-t	object_subtype	Obligatoire. Type de tâche ou de transformation auquel vous donnez un libellé. <i>pmrep</i> ignore les autres types d'objets. Pour plus d'informations sur les sous-types valides, consultez "Liste des types d'objets" à la page 1433 .
-v	version_number	Facultatif. Version de l'objet auquel appliquer le libellé. La commande échoue si la version est extraite. Applique par défaut le libellé à la dernière version de l'objet.
-f	folder_name	Facultatif. Dossier qui contient les objets. Si vous entrez un nom de dossier, mais aucun nom d'objet, <i>pmrep</i> applique le libellé à tous les objets du dossier. Si vous entrez un nom de dossier avec un nom d'objet, <i>pmrep</i> cherche l'objet dans le dossier. Vous ne pouvez pas utiliser l'option -f si vous utilisez l'option -i.
-i	persistent_input_file	Facultatif. Nom d'un fichier texte généré à partir de ExecuteQuery, ListObjectDependency ou Validate. Contient une liste des objets destinés à recevoir le libellé. Si vous utilisez cette option, n'utilisez pas le nom d'objet, le type d'objet ou le nom de dossier pour spécifier les objets.
-d	dependency_object_types	Facultatif. Types d'objets dépendant auxquels donner un libellé. Les types d'objets dépendants valides comprennent les raccourcis, les mappages, les mapplets, les sessions, les flux de travail, les worklets, les définitions cibles, les définitions sources et les dépendances de clé étrangère. Utilisez cette option avec l'option -p. Si vous entrez un type d'objet, le libellé s'applique aux objets dépendants de ce type d'objet.
-p	dependency_direction	Facultatif. Parents ou enfants dépendants auxquels appliquer le libellé. Vous pouvez spécifier des parents, des enfants ou les deux. Si vous n'entrez pas l'option -d, tous les objets dépendants reçoivent le libellé. Si vous n'entrez pas cette option, le libellé s'applique à l'objet spécifié.

Option	Argument	Description
-s	-	Facultatif. Inclure les objets de dépendance clé primaire et clé étrangère indépendamment de la direction de la dépendance.
-g	-	Facultatif. Trouver les dépendances des objets entre les référentiels.
-m	-	Facultatif. Déplacer un libellé depuis la version actuelle vers la dernière version d'un objet. Utilisez cet argument lorsque le type de libellé est one_per_object.
-c	commentaires	Facultatif. Commentaires sur le libellé.
-e	dbd_separator	Facultatif. Si une source ODBC comporte un point (.) dans le nom, définissez un autre caractère de séparation lorsque vous définissez l'objet source. Par exemple, au lieu de database_name.source_name, définissez l'objet source comme database_name\source_name et définissez dbd_separator comme une barre oblique inversée (\).

AssignIntegrationService

Attribue le service d'intégration PowerCenter au flux de travail spécifié.

Si vous exécutez le flux de travail à partir du gestionnaire de flux de travail et lui associez un service d'intégration PowerCenter dans la commande *pmrep AssignIntegrationService*, le flux de travail s'exécute sur le service d'intégration PowerCenter spécifié avec l'option -i.

Si vous exécutez le flux de travail à partir de la ligne de commande, il s'exécute sur le service d'intégration PowerCenter spécifié dans la commande *pmcmd StartWorkflow*. Le flux de travail n'est pas exécuté sur le service d'intégration PowerCenter que vous avez spécifié dans la commande *pmrep AssignIntegrationService*.

La commande AssignIntegrationService utilise la syntaxe suivante :

```
assignintegrationsservice
-f <folder_name>
-n <workflow_name>
-i <integration_service_name>
```

Le tableau suivant décrit les options et les arguments de *pmrep AssignIntegrationService* :

Option	Argument	Description
-f	folder_name	Requis. Nom du dossier qui contient le flux de travail. Pour saisir un nom qui contient un espace ou un autre caractère non alphanumérique, placez-le entre guillemets.
-n	workflow_name	Requis. Nom du flux de travail.
-i	nom_service_d'intégration	Requis. Nom du service d'intégration PowerCenter associé au flux de travail.

AssignPermission

Vous permet d'ajouter, de supprimer ou de mettre à jour des autorisations sur un objet global pour un utilisateur, un groupe ou pour le groupe par défaut Others.

Remarque: Seuls l'administrateur ou le propriétaire actuel de l'objet peuvent gérer les autorisations de l'objet.

La commande AssignPermission utilise la syntaxe suivante :

```
AssignPermission  
-o <object_type>  
[-t <object_subtype>]  
-n <object_name>  
{-u <user_name> | -g <group_name>}  
[-s <security_domain>]  
-p <permission>
```

Le tableau suivant décrit les options et arguments de la commande *pmrep* AssignPermission :

Option	Argument	Description
-o	object_type	Obligatoire. Type de l'objet pour lequel vous voulez gérer les autorisations. Vous pouvez spécifier dossier, libellé, groupe de déploiement, requête ou connexion.
-t	object_subtype	Facultatif. Type d'objet de connexion ou de requête. Non obligatoire pour les autres types d'objets. Pour plus d'informations sur les sous-types valides, consultez "AssignPermission" à la page 1392 .
-n	object_name	Requis. Nom de l'objet pour lequel vous voulez gérer les autorisations. Vous pouvez utiliser des caractères spéciaux pour le nom de l'objet.
-u	user_name	Obligatoire si vous n'utilisez pas l'option -g. Nom de l'utilisateur pour lequel vous souhaitez ajouter, supprimer ou mettre à jour des autorisations. Utilisez l'option -u ou -g, mais pas les deux.
-g	group_name	Nom du groupe pour lequel vous voulez ajouter, supprimer ou mettre à jour des autorisations. Spécifiez « Autres » comme nom de groupe pour modifier les autorisations du groupe par défaut Autres. Utilisez l'option -u ou -g, mais pas les deux. Vous pouvez utiliser des caractères spéciaux pour le nom du groupe.
-s	security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur ou le groupe. La valeur par défaut est Natif.
-p	autorisation	Requis. Autorisations que vous voulez ajouter, supprimer ou mettre à jour. Vous attribuez des autorisations de lecture, d'écriture et d'exécution sur un objet global. Utilisez les caractères r, w et x pour attribuer des autorisations de lecture, d'écriture et d'exécution.

Le tableau suivant décrit les types d'objets et les valeurs à utiliser avec les commandes *pmrep* :

Type d'objet	Sous-type d'objet
Requête	Partagé
Requête	Personnel
Connexion	Application
Connexion	FTP
Connexion	Chargeur
Connexion	File d'attente
Connexion	Relationnel

Exemple

Vous pouvez ajouter, supprimer ou mettre à jour des autorisations avec l'option -p.

Par exemple, pour ajouter des autorisations de lecture et d'écriture à un dossier, entrez le texte suivant à l'invite :

```
pmrep AssignPermission -o folder -n Sales -u Admin -p rw
```

Vous pouvez également mettre à jour des autorisations sur un objet. Par exemple, vous avez assigné l'autorisation de lecture sur un dossier et devez ajouter l'autorisation d'écriture. Pour mettre à jour les autorisations, entrez le texte suivant à l'invite :

```
pmrep AssignPermission -o folder -n Sales -u Admin -p rw
```

Pour mettre à jour toutes les autorisations, entrez le texte suivant à l'invite :

```
pmrep AssignPermission -o folder -n Sales -u Admin -p ""
```

BackUp

Sauvegarde du référentiel vers le fichier spécifié avec l'option -o. Vous devez fournir le nom du fichier de sauvegarde. Utilisez cette commande lorsque le référentiel est en cours d'exécution. Vous devez être connecté à un référentiel pour utiliser cette commande.

La commande BackUp utilise la syntaxe suivante :

```
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)]
```

Le tableau suivant décrit les options et arguments de *pmrep* BackUp :

Option	Argument	Description
-o	output_file_name	Obligatoire. Nom et chemin du fichier de sauvegarde du référentiel. Lorsque vous affichez la liste des fichiers de sauvegarde du référentiel dans l'outil Administrator, vous ne pouvez voir que les fichiers ayant une extension .rep.
-d	description	Facultatif. Crée une description du fichier de sauvegarde en fonction de la chaîne qui suit l'option. Le processus de sauvegarde tronque tout caractère au-delà de 2 000.
-f	-	Facultatif. Écrase un fichier existant ayant le même nom.
-b	-	Facultatif. Ignore les tables associées au flux de travail et les journaux de session pendant la sauvegarde.
-j	-	Facultatif. Ignore l'historique du groupe de déploiement pendant la sauvegarde.
-q	-	Facultatif. Ignore les tables associées aux données MX pendant la sauvegarde.
-v	-	Facultatif. Ignore les statistiques pendant la sauvegarde.

Pour restaurer le fichier de sauvegarde, utilisez l'outil Administrator ou utilisez la commande *pmrep* Restore.

ChangeOwner

Modifie le nom du propriétaire d'un objet global.

Remarque: Seuls l'administrateur ou le propriétaire actuel de l'objet ont l'autorisation de changer le propriétaire d'un objet.

La commande ChangeOwner utilise la syntaxe suivante :

```
ChangeOwner  
-o <object_type>  
[-t <object_subtype>]  
-n <object_name>  
-u <new_owner_name>  
[-s <security_domain>]
```

Le tableau suivant décrit les options et arguments de *pmrep* ChangeOwner :

Option	Argument	Description
-o	object_type	Obligatoire. Type de l'objet. Vous pouvez spécifier dossier, libellé, groupe de déploiement, requête ou connexion.
-t	object_subtype	Facultatif. Type de demande d'objet ou d'objet de connexion. Non obligatoire pour les autres types d'objets. Pour plus d'informations sur les sous-types valides, consultez "AssignPermission" à la page 1392 .
-n	object_name	Requis. Nom de l'objet. Vous pouvez utiliser des caractères spéciaux pour le nom de l'objet.
-u	new_owner_name	Obligatoire. Nom du nouveau propriétaire. Le nom du nouveau propriétaire doit être un compte utilisateur valide dans le domaine.
-s	security_domain	Obligatoire si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient le nouveau propriétaire. La valeur par défaut est Natif.

CheckIn

Archive un objet que vous avez extrait. Lorsque vous archivez un objet, le référentiel crée une nouvelle version de l'objet et lui assigne un numéro de version. Le numéro de version est un nombre supérieur au numéro de la dernière version archivée.

La commande CheckIn utilise la syntaxe suivante :

```
checkin  
-o <object_type>  
[-t <object_subtype>]  
-n <object_name>  
-f <folder_name>  
[-c <comments>]  
[-s dbd_separator]
```

Le tableau suivant décrit les options et arguments de *pmrep* CheckIn :

Option	Argument	Description
-o	object_type	Obligatoire. Type d'objet que vous archivez : source, cible, transformation, mappage, session, worklet, flux de travail, planificateur, configuration de session, tâche, cube ou dimension.
-t	object_subtype	Facultatif. Type de tâche ou de transformation à archiver. Pas obligatoire pour les autres types d'objets. Pour plus d'informations sur les sous-types valides, consultez "Liste des types d'objets" à la page 1433 .
-n	object_name	Obligatoire. Nom de l'objet que vous archivez.

Option	Argument	Description
-f	folder_name	Obligatoire. Dossier destiné à contenir la nouvelle version de l'objet.
-c	commentaires	Facultatif. Commentaires sur l'archivage.
-s	dbd_separator	Facultatif. Si une source ODBC comporte un point (.) dans le nom, définissez un autre caractère de séparation lorsque vous définissez l'objet source. Par exemple, au lieu de database_name.source_name, définissez l'objet source comme database_name\source_name et définissez dbd_separator comme une barre oblique inversée (\).

CleanUp

Nettoie toute ressource persistante créée par *pmrep*. Cette commande nettoie également toute information de connexion des précédentes sessions de *pmrep*. Appeler la commande CleanUp comme première commande dans une session renvoie toujours une erreur.

Si vous appelez CleanUp en mode interactif, *pmrep* se déconnecte de tout référentiel auquel vous êtes connecté.

La commande CleanUp utilise la syntaxe suivante :

```
cleanup
```

ClearDeploymentGroup

Efface tous les objets d'un groupe de déploiement. Utilisez cette commande pour conserver le groupe de déploiement, mais en retirer les objets.

La commande ClearDeploymentGroup utilise la syntaxe suivante :

```
cleardeploymentgroup
-p <deployment_group_name>
[-f (force clear)]
```

Le tableau suivant décrit les options et arguments de *pmrep* ClearDeploymentGroup :

Option	Argument	Description
-p	deployment_group_name	Obligatoire. Nom du groupe de déploiement que vous voulez nettoyer.
-f	-	Facultatif. Supprime les objets sans confirmation. Si vous omettez cet argument, la commande vous demande confirmation avant d'effacer les objets.

Connect

Se connecte à un référentiel. La première fois que vous utilisez pmrep en mode ligne de commande ou en mode interactif, vous devez utiliser la commande Connect. Toutes les commandes requièrent une connexion au référentiel sauf les commandes suivantes :

- Exit
- Aide
- ListAllPrivileges

En mode ligne de commande, pmrep utilise les informations spécifiées par le dernier appel pour se connecter au référentiel. Si pmrep est appelé sans connexion réussie, la commande renvoie une erreur. En mode ligne de commande, pmrep se connecte et se déconnecte du référentiel à chaque commande.

Pour utiliser pmrep afin d'effectuer des tâches dans plusieurs référentiels au cours d'une seule session, vous devez exécuter la commande Connect à chaque fois que vous voulez passer à un autre référentiel. En mode interactif, pmrep maintient la connexion jusqu'à ce que vous quittiez pmrep ou jusqu'à ce que vous vous connectiez à nouveau. Si vous rappelez Connect, pmrep se déconnecte du premier référentiel et se connecte ensuite au second référentiel. Si la seconde connexion échoue, la connexion précédente reste déconnectée et vous ne serez connecté à aucun référentiel. Si vous exécutez une commande qui requiert une connexion au référentiel et que vous n'êtes pas connecté à ce référentiel, pmrep utilise les informations de connexion spécifiées lors de la dernière connexion réussie au référentiel depuis n'importe quelle session antérieure de pmrep. pmrep conserve les informations de la dernière connexion réussie jusqu'à ce que vous utilisiez la commande Cleanup.

La commande Connect utilise la syntaxe suivante :

```
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>]
```

Le tableau suivant décrit les options et arguments de pmrep Connect :

Option	Argument	Description
-r	repository_name	Obligatoire. Nom du référentiel auquel vous souhaitez être connecté.
-d	domain_name	Obligatoire si vous n'utilisez pas -h et -o. Nom du domaine du référentiel. Si vous utilisez l'option -d, n'utilisez pas les options -h et -o.

Option	Argument	Description
-h	portal_host_name	Obligatoire si vous n'utilisez pas -d. Si vous utilisez l'option -h, vous devez également utiliser l'option -o. Nom de l'hôte de passerelle.
-o	portal_port_number	Obligatoire si vous n'utilisez pas -d. Si vous utilisez l'option -o, vous devez également utiliser l'option -h. Numéro de port de passerelle.
-n	user_name	Facultatif. Nom d'utilisateur utilisé pour la connexion au référentiel.
-s	user_security_domain	Requis si vous utilisez l'authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. La valeur par défaut est Natif.
-x	password	Obligatoire si vous utilisez l'option -n et que vous n'utilisez pas l'option -X. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Utilisez l'option -x ou -X, mais pas les deux.
-X	password_environment_variable	Obligatoire si vous utilisez l'option -n et que vous n'utilisez pas l'option -x. Variable d'environnement de mot de passe. Utilisez l'option -x ou -X, mais pas les deux.
-u	connect_without_user_in_kerberos_mode	Obligatoire. Se connecte à un service de référentiel sans nom d'utilisateur et mot de passe lorsque le domaine Informatica utilise l'authentification Kerberos. Utilisez l'option -u pour vous connecter au service de référentiel si le référentiel n'a pas de contenu.
-t	client_resilience	Facultatif. Durée en secondes pendant laquelle pmrep tente d'établir ou de rétablir une connexion au référentiel. Si vous omettez l'option -t, pmrep utilise la valeur de dépassement de délai spécifiée dans la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si aucune valeur n'est spécifiée dans la variable d'environnement, la valeur par défaut de 180 secondes est utilisée.

Créer

Crée les tables du référentiel dans la base de données. Avant de pouvoir créer les tables du référentiel, vous devez effectuer ces tâches :

- Créez et configurez la base de données destinée à contenir le référentiel.
- Créez le service de référentiel dans l'outil Administrator ou avec *infacmd*.
- Exécutez le service de référentiel en mode exclusif dans l'outil Administrator ou avec *infacmd*.
- Connectez-vous au référentiel dans *pmrep*.

Vous ne pouvez pas utiliser la commande Create si la base de données du référentiel contient déjà des tables de référentiel.

Pour utiliser la commande Create, vous devez avoir l'autorisation sur le service de référentiel dans le domaine.

La commande Create utilise la syntaxe suivante :

```
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)]
```

Le tableau suivant décrit les options et arguments de *pmrep* Create :

Option	Argument	Description
-u	domain_user_name	Obligatoire. Nom d'utilisateur.
-s	domain_user_security_domain	Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. La valeur par défaut est Natif.
-p	domain_password	Facultatif. Mot de passe. Utilisez l'option -p ou -P, mais pas les deux. Si vous n'utilisez ni l'option -p ni l'option -P, <i>pmrep</i> vous invite à entrer le mot de passe.
-P	domain_password_environment_variable	Facultatif. Variable d'environnement de mot de passe. Utilisez l'option -p ou -P, mais pas les deux. Si vous n'utilisez ni l'option -p ni l'option -P, <i>pmrep</i> vous invite à entrer le mot de passe.
-g	-	Facultatif. Effectue la promotion du référentiel vers un référentiel global.
-v	-	Facultatif. Active le versionnage de l'objet pour le référentiel.

CreateConnection

Crée une connexion source ou cible dans le référentiel. La connexion peut être une connexion relationnelle, d'application ou FTP. Les connexions à la base de données relationnelle de chaque sous-type relationnel exigent un sous-ensemble de toutes les options et de tous les arguments de CreateConnection. Par exemple, les connexions Oracle n'acceptent pas les options -z, -d ou -t. Utilisez l'option -k pour spécifier des attributs des connexions d'application.

La commande CreateConnection utilise la syntaxe suivante :

```
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)]
```

Le tableau suivant décrit les options et arguments de *pmrep* CreateConnection :

Option	Argument	Description
-s	connection_subtype	Requis. Affiche le sous-type de connexion. Les types de connexion sont les suivants : - Application - FTP - Relationnel Par exemple, pour une connexion relationnelle, les sous-types de connexion comprennent Oracle, Sybase et Microsoft SQL Server. Pour les connexions FTP, le sous-type valide est FTP.
-n	connection_name	Requis. Nom de la connexion.
-u	user_name	Requis pour certains types de connexion. Nom d'utilisateur utilisé pour l'authentification.
-p	mot de passe	Requis pour certains types de connexion. Mot de passe utilisé pour l'authentification lorsque vous vous connectez à la base de données relationnelle. Utilisez l'option -p ou -P, mais pas les deux. Si vous spécifiez un nom d'utilisateur sans indiquer -p ou -P, <i>pmrep</i> vous demande le mot de passe. Pour spécifier un paramètre dans le mot de passe, ajoutez le préfixe \$Param dans l'option -p et veillez à utiliser l'option -w. N'utilisez pas de signe dollar (\$) ailleurs dans l'option -p et entrez le mot de passe du paramètre sans espace. Par exemple, -p '\$Param_abc' -w
-P	password_environment_variable	Facultatif. Variable d'environnement de mot de passe utilisée pour l'authentification lorsque vous vous connectez à la base de données relationnelle. Utilisez l'option -p ou -P, mais pas les deux. Si vous n'utilisez ni l'option -p, ni l'option -P, <i>pmrep</i> vous demande le mot de passe.
-w	-	Facultatif. Vous permet d'utiliser un paramètre dans l'option de mot de passe. <i>pmrep</i> utilise le mot de passe spécifié avec l'option -p ou -P comme nom du paramètre de session au moment de l'exécution. Valide uniquement si vous utilisez l'option -p ou -P. Si vous n'utilisez pas de paramètre dans l'option de mot de passe, <i>pmrep</i> utilise le mot de passe d'utilisateur spécifié avec l'option -p ou -P.
-K	connection_to_the_Kerberos_server	Facultatif. Indique que la base de données à laquelle vous vous connectez s'exécute sur un réseau qui utilise l'authentification Kerberos.
-c	connect_string	Chaîne de connexion utilisée par le service d'intégration pour se connecter à la base de données relationnelle.
-l	code_page	Requis pour certains types de connexion. Page de code associée à la connexion.
-r	rollback_segment	Facultatif. Valide pour les connexions Oracle. Nom du segment de retour arrière. Un segment de retour arrière enregistre les transactions de la base de données qui vous permettent d'annuler la transaction.

Option	Argument	Description
-e	connection_ environment_sql	Facultatif. Commandes SQL permettant de définir l'environnement de base de données lorsque vous vous connectez à la base de données. Le service d'intégration exécute l'environnement SQL de connexion à chaque fois qu'il se connecte à la base de données.
-f	transaction_ environment_sql	Facultatif. Commandes SQL permettant de définir l'environnement de base de données lorsque vous vous connectez à la base de données. Le service d'intégration exécute l'environnement de transaction SQL au début de chaque transaction.
-z	packet_size	Facultatif. Valide pour les connexions Sybase ASE et Microsoft SQL Server. Optimise la connexion ODBC pour Sybase ASE et Microsoft SQL Server.
-b	database_name	Facultatif. Nom de la base de données. Valide pour les connexions Sybase ASE et Microsoft SQL Server.
-v	server_name	Nom facultatif du serveur de base de données. Valide pour les connexions Sybase ASE et Microsoft SQL Server.
-d	domain_name	Facultatif, valide pour les connexions Microsoft SQL Server. Nom du domaine. Utilisé par Microsoft SQL Server.
-t	-	Facultatif. Valide pour les connexions Microsoft SQL Server. Si cette option est activée, le service d'intégration utilise l'authentification Windows pour accéder à la base de données Microsoft SQL Server. Le nom d'utilisateur qui démarre le service d'intégration doit être celui d'un utilisateur Windows valide ayant accès à la base de données Microsoft SQL Server.
-a	data_source_name	Nom facultatif de la source de données ODBC Teradata. Valide pour les connexions Teradata.
-x	-	Active la sécurité renforcée. Vous attribue les autorisations d'accès en lecture, d'accès en écriture et d'exécution. Les groupes Public et Monde n'ont aucune autorisation. Si cette option n'est pas activée, les autorisations d'accès en lecture, d'accès en écriture et d'exécution sont accordées à tous les groupes et à tous les utilisateurs.
-k	connection_attributes	Active les attributs de connexion définis par l'utilisateur. Le format des attributs est le suivant : <nom>=<valeur>;<nom>=<valeur>. Remarque: N'ajoutez pas d'espace devant le nom de l'attribut.
-y	-	Active la valeur de type de fournisseur. Vous pouvez sélectionner les types de fournisseur suivants : - 1 pour ODBC - 2 pour Oledb (déconseillé)

Option	Argument	Description
-m	-	Active l'attribut Utiliser DSN. Le service d'intégration PowerCenter récupère les noms de serveur et de base de données depuis le DSN.
-S	odbc_subtype	Facultatif. Active le sous-type ODBC pour une connexion ODBC. Une connexion ODBC peut être l'un des sous-types ODBC suivants : <ul style="list-style-type: none"> - AWS Redshift - Azure DW - Greenplum - Google BigQuery - PostgreSQL - Snowflake - SAP HANA - Aucun La valeur par défaut est Aucun.

Pour plus d'informations sur les sous-types de connexion, consultez ["Sous-types de connexion" à la page 1384](#).

Spécification de la page de code de la base de données

L'option -l spécifie la page de code pour la connexion à la base de données. Entrez le nom de la page de code que vous voulez assigner à la connexion de base de données. Par exemple, pour affecter la page de code US-ASCII à la connexion de base de données, entrez le nom de page de code « US-ASCII ».

Modifier la page de code de connexion à la base de données peut entraîner des données incohérentes si la nouvelle page de code n'est pas compatible avec les pages de code source ou cible de connexion à la base de données. En outre, si vous configurez le service d'intégration des données pour valider la page de code, changer la page de code de connexion à la base de données peut entraîner l'échec des sessions si la page de code source de connexion à la base de données n'est pas un sous-ensemble de la page de code cible de connexion à la base de données.

CreateDeploymentGroup

Crée un groupe de déploiement. Vous pouvez créer un groupe de déploiement dynamique ou statique. Pour créer un groupe de déploiement dynamique, vous devez fournir un nom de requête et indiquer si la requête est privée ou publique.

La commande CreateDeploymentGroup utilise la syntaxe suivante :

```
createdeploymentgroup
-p <deployment_group_name>
[-t <deployment_group_type (static or dynamic)>]
[-q <query_name>]
[-u <query_type (shared or personal)>]
[-c <comments>]
```

Le tableau suivant décrit les options et arguments de *pmrep* `CreateDeploymentGroup` :

Option	Argument	Description
-p	deployment_group_name	Obligatoire. Nom du groupe de déploiement à créer.
-t	deployment_group_type	Facultatif. Créez un groupe statique ou utilisez une requête pour créer le groupe dynamiquement. Vous pouvez spécifier static ou dynamic. La valeur par défaut est static.
-q	query_name	Obligatoire si le groupe de déploiement est dynamique, mais ignoré si le groupe est statique. Nom de la requête associée au groupe de déploiement.
-u	query_type	Obligatoire si le groupe de déploiement est dynamique, mais ignoré si le groupe est statique. Type de requête pour créer un groupe de déploiement. Vous pouvez spécifier shared ou personal.
-c	commentaires	Facultatif. Commentaires sur le nouveau groupe de déploiement.

CreateFolder

Crée un dossier dans le référentiel.

La commande `CreateFolder` utilise la syntaxe suivante :

```
createfolder  
-n <folder_name>  
[-d <folder_description>]  
[-o <owner_name>]  
[-a <owner_security_domain>]  
[-s (shared_folder)]  
[-p <permissions>]  
[-f <active | frozendeploy | frozennodeploy>]
```

Le tableau suivant décrit les options et arguments de *pmrep* `CreateFolder` :

Option	Argument	Description
-n	folder_name	Obligatoire. Nom du dossier.
-d	folder_description	Facultatif. Description du dossier qui apparaît dans le gestionnaire du référentiel. Si la description du dossier contient des espaces ou d'autres caractères non alphanumériques, placez-la entre guillemets.
-o	owner_name	Facultatif. Propriétaire du dossier. N'importe quel utilisateur du référentiel peut être le propriétaire du dossier. Le propriétaire par défaut est l'utilisateur à l'origine de la création du dossier.

Option	Argument	Description
-a	owner_security_domain	Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient le propriétaire. La valeur par défaut est Natif.
-s	-	Facultatif. Partage le dossier.
-p	autorisations	Facultatif. Droits d'accès au dossier. Si cette option est omise, le service de référentiel assigne les autorisations par défaut.
-f	actif frozendeploy frozenodeploy	Facultatif. Modifie le statut du dossier par l'un des statuts suivants : <ul style="list-style-type: none"> - actif. Ce statut permet d'extraire des objets avec version dans le dossier. - frozendeploy (Gelé, Permettre Déploiement pour Remplacer). Ce statut empêche les utilisateurs d'archiver des objets dans le dossier. Le déploiement dans le dossier crée de nouvelles versions des objets. - frozenodeploy (Gelé, ne pas permettre Déploiement pour Remplacer). Ce statut empêche les utilisateurs d'archiver des objets dans le dossier. Vous ne pouvez pas déployer d'objets dans ce dossier.

Remarque: Vous pouvez ajouter, supprimer ou mettre à jour les autorisations d'un dossier en utilisant la commande AssignPermission.

Attribution des autorisations

Vous pouvez affecter des autorisations au propriétaire, au groupe et au référentiel en entrant trois chiffres lorsque vous utilisez l'option -p. Le premier chiffre correspond aux autorisations du propriétaire, le second aux autorisations du groupe auquel appartient l'utilisateur et le troisième correspond à toutes les autres autorisations.

Entrez un nombre pour chaque ensemble d'autorisations. Chaque autorisation est associée à un nombre. Désignez 4 pour une autorisation de lecture, 2 pour une autorisation d'écriture et 1 pour une autorisation d'exécution. Pour assigner des autorisations, entrez 4, 2, 1 ou la somme de n'importe lesquels de ces chiffres.

Par exemple, si vous voulez assigner les autorisations par défaut, utilisez la syntaxe de commande suivante :

```
-p 764
```

Ceci donne au propriétaire du dossier les autorisations de lecture, écriture et exécution (7 = 4+2+1). Le groupe du propriétaire a les autorisations en lecture et écriture (6 = 4+2). Tous les autres ont l'autorisation de lecture.

La commande renvoie le message « commande CreateFolder correctement terminée » ou « échec de la commande CreateFolder ». La création peut échouer pour les raisons suivantes :

- Le dossier existe déjà.
- Le propriétaire n'existe pas ou n'appartient pas au groupe.

CreateLabel

Crée un libellé que vous utilisez pour associer des groupes d'objets lors du développement. Vous pouvez associer un libellé avec n'importe quel objet avec version ou groupe d'objets dans un référentiel.

La commande CreateLabel utilise la syntaxe suivante :

```
createlabel  
-a <label_name>  
[-c <comments>]
```

Le tableau suivant décrit les options et arguments de *pmrep* CreateLabel :

Option	Argument	Description
-a	label_name	Obligatoire. Nom du libellé que vous créez.
-c	commentaires	Facultatif. Commentaires sur le libellé.

CreateQuery

Crée une demande d'objet dans le référentiel. Vous devez configurer les conditions de requête pour créer une demande d'objet. Une condition de requête se compose d'un paramètre, d'un opérateur et d'une valeur. Vous pouvez entrer l'expression dans un fichier ou à l'invite de commandes.

La commande CreateQuery utilise la syntaxe suivante :

```
createquery  
-n <query_name>  
-t <query_type (shared or personal)>  
{-e <expression> |  
-f <file_name>}  
[-u (UTF-8 encoded input file)]  
[-c <comments>]
```

Le tableau suivant décrit les options et arguments de la commande *pmrep* CreateQuery :

Option	Argument	Description
-n	query_name	Requis. Nom de la requête que vous voulez créer.
-t	query_type	Requis. Type de requête. Vous pouvez spécifier shared ou personal.
-e	expression	Requis si vous n'utilisez pas l'option -f. Expression de la requête.
-f	file_name	Requis si vous n'utilisez pas l'option -e. Nom et chemin d'accès du fichier contenant l'expression d'une requête. Vous devez utiliser l'option -e ou -f, mais pas les deux.

Option	Argument	Description
-u	-	Facultatif. Encode le fichier au format UTF-8. Remarque : si vous ne spécifiez pas l'option -u, le codage système par défaut encode le fichier.
-c	comments	Facultatif. Commentaires sur la requête.

Le tableau suivant décrit les paramètres de requête ainsi que les opérateurs et valeurs valides pour chaque paramètre :

Paramètre	Description	Opérateur valide	Valeurs acceptées
BusinessName	Affiche les sources et cibles en fonction de leurs noms d'entreprise. Par exemple, le nom d'entreprise de la requête est égal (Equals) à Informatica, retourne les sources et cibles contenant le nom d'entreprise Informatica et filtre tous les autres objets.	Contains, EndsWith, Equals, In, Not Contains, Not Equals, Not EndsWith, Not In, Not StartsWith, StartsWith	Chaîne
CheckinTime	Affiche les objets avec version archivés sur une période spécifiée, avant ou après une période spécifiée ou dans un nombre de jours spécifié. Vous ne pouvez spécifier ce paramètre que pour les référentiels avec version.	Between, GreaterThan, LessThan, Not Between, WithinLastDays	Date/heure, Numérique
CheckoutTime	Affiche les objets avec version extraits sur une période spécifiée, avant ou après une période spécifiée ou dans un nombre de jours spécifié. Vous ne pouvez spécifier ce paramètre que pour les référentiels avec version.	Between, GreaterThan, LessThan, Not Between, WithinLastDays	Date/heure, Numérique
Comments	Affiche les commentaires associés à une source, une cible, un mappage ou un flux de travail.	Contains, Equals, EndsWith, In, Not Contains, Not Equals, Not EndsWith, Not In, Not StartsWith, StartsWith	Chaîne

Paramètre	Description	Opérateur valide	Valeurs acceptées
DeploymentDispatchHistory	Affiche les objets avec version déployés sur un autre dossier ou référentiel à l'aide des groupes de déploiement sur une période donnée.	Between, GreaterThan, LessThan, Not Between, WithinLastDays	Date/heure, Numérique
DeploymentReceiveHistory	Affiche les objets avec version déployés depuis un autre dossier ou référentiel à l'aide de groupes de déploiement sur une période donnée.	Between, GreaterThan, LessThan, Not Between, WithinLastDays	Date/heure, Numérique
Dossier	Affiche les objets dans un dossier spécifique.	Equals, In, Not Equals, Not In	Nom du dossier
IncludeChildren	Affiche les objets dépendants enfant.	Où (Valeur 1) dépend de (Valeur 2), (Valeur 3)	Pour la valeur 1 et la valeur 2, utilisez : Quelconque, Définition de source, Définition de cible, Transformation, Mapplet, Mappage, Cube, Dimension, Tâche, Session, Worklet, Flux de travail, Planificateur, SessionConfig Pour la valeur 3, utilisez : Dépendance non réutilisable, Dépendance réutilisable.

Paramètre	Description	Opérateur valide	Valeurs acceptées
IncludeChildrenAndParents	Affiche les objets dépendants enfant et parent.	Où (Valeur 1) dépend de (Valeur 2), (Valeur 3)	Pour la valeur 1 et la valeur 2, utilisez : Quelconque, Définition de source, Définition de cible, Transformation, Mapplet, Mappage, Cube, Dimension, Tâche, Session, Worklet, Flux de travail, Planificateur, SessionConfig Pour la valeur 3, utilisez : Dépendance non réutilisable, Dépendance réutilisable.
IncludeParents	Affiche les objets dépendants parent.	Où (Valeur 1) dépend de (Valeur 2), (Valeur 3)	Pour la valeur 1 et la valeur 2, utilisez : Quelconque, Définition de source, Définition de cible, Transformation, Mapplet, Mappage, Cube, Dimension, Tâche, Session, Worklet, Flux de travail, Planificateur, SessionConfig Pour la valeur 3, utilisez : Dépendance non réutilisable, Dépendance réutilisable.
IncludePKFKDependencies	Affiche les dépendances de clé primaire-clé étrangère.	-	-

Paramètre	Description	Opérateur valide	Valeurs acceptées
ImpactedStatus	Affiche les objets en fonction du statut « Concerné ». Les objets peuvent être marqués comme étant concernés lorsqu'un objet enfant change de telle manière que l'objet parent peut ne pas être en mesure de s'exécuter.	Equals	Concerné, Non concerné
Label	Affiche les objets avec version associés à une étiquette ou un groupe d'étiquettes. Vous ne pouvez spécifier ce paramètre que pour les référentiels avec version.	Contains, Equals, EndsWith, In, Not Contains, Not Equals, Not EndsWith, In, Not StartsWith, Not In, StartsWith	Chaîne
LastSavedTime	Affiche les objets enregistrés à un moment particulier ou au cours d'une période particulière.	Between, GreaterThan, LessThan, Not Between, WithinLastDays	Date/heure, Numérique
LatestStatus	Affiche les objets avec version basés sur l'historique d'objet. La requête peut retourner des objets locaux extraits, la dernière version des objets archivés ou une collection de toutes les anciennes versions des objets. Vous ne pouvez spécifier ce paramètre que pour les référentiels avec version.	Equals, Not Equals, In	Checked-out Latest, Checked-in Older
MetadataExtension	Affiche les objets en fonction d'un nom d'extension ou d'une paire de valeurs. Utilisez ce paramètre de requête pour rechercher des extensions de métadonnées non réutilisables. La requête ne retourne pas les extensions de métadonnées réutilisables définies par l'utilisateur.	Equals, Not Equals	Domaine de métadonnées défini par le fournisseur

Paramètre	Description	Opérateur valide	Valeurs acceptées
ObjectName	Affiche les objets en fonction du nom d'objet.	Contains, Equals, EndsWith, In, Not Contains, Not Equals, Not EndsWith, Not StartsWith, Not In, StartsWith	Chaîne
ObjectType	Affiche les objets en fonction du type d'objet. Par exemple, vous pouvez rechercher tous les flux de travail dans un dossier spécifié.	Equals, In, Not Equals, Not In	Cube, Dimension, Mappage, Mapplet, Planificateur, Session, Configuration de session, Définition de source, Définition de cible, Tâche, Transformation, Fonction définie par l'utilisateur, Flux de travail, Worklet
ObjectUsedStatus	Affiche les objets utilisés par d'autres objets. Par exemple, vous pouvez rechercher des mappages non utilisés dans une session. Si une quelconque version d'un objet est utilisée par un autre objet, la requête retourne la version la plus récente de l'objet, même lorsque celle-ci est inutilisée. La requête ne retourne pas de flux de travail ou de cubes car ces objets ne peuvent pas être utilisés par d'autres objets.	Equals	Non utilisé, Utilisé

Paramètre	Description	Opérateur valide	Valeurs acceptées
ShortcutStatus	Affiche les objets en fonction du statut « Raccourci ». Si vous sélectionnez cette option, la requête retourne des objets de raccourci locaux et globaux. Les objets de raccourci sont considérés comme valides sans tenir compte du fait que les objets qu'ils référencent soient ou non valides.	Equals	N'est pas un raccourci, Est un raccourci
Reusable Status	Affiche les objets réutilisables ou non réutilisables.	Equals, In	Non réutilisable, Réutilisable
User	Affiche les objets archivés ou extraits par l'utilisateur spécifié.	Equals, In, Not Equals, Not In	Utilisateurs dans le référentiel spécifié
ValidStatus	Affiche les objets valides ou non valides. Le service de référentiel valide un objet lorsque vous exécutez la validation ou enregistrez un objet dans le référentiel.	Equals	Non valide, Valide
VersionStatus	Affiche les objets en fonction du statut « Supprimé » ou « Non supprimé ». Vous ne pouvez spécifier ce paramètre que pour les référentiels avec version.	Equals, In	Supprimé, Non supprimé

Supprimer

Supprime les tables du référentiel de la base de données du référentiel.

Avant d'utiliser la commande Delete, vous devez vous connecter au référentiel et lui fournir un nom d'utilisateur et un mot de passe ou la variable d'environnement de mot de passe.

Lorsque vous utilisez la commande Delete, le service de référentiel doit être exécuté en mode exclusif. Vous pouvez configurer le service de référentiel pour qu'il s'exécute en mode exclusif dans l'outil Administrator ou vous pouvez utiliser la commande *infacmd* UpdateRepositoryService.

La commande Delete utilise la syntaxe suivante :

```
delete
[-x <repository_password_for_confirmation> |
-X <repository_password_environment_variable_for_confirmation>]
[-f (forceful delete: unregisters local repositories and deletes)]
```


Le tableau suivant décrit les options et arguments de *pmrep Delete* :

Option	Argument	Description
-x	repository_password_for_confirmation	Facultatif. Mot de passe. Vous pouvez utiliser l'option -x ou -X, mais pas les deux. Si vous n'utilisez ni l'option -x, ni l'option -X, <i>pmrep</i> vous demande une confirmation du mot de passe.
-X	repository_password_environment_variable_for_confirmation	Facultatif. Variable d'environnement de mot de passe. Vous pouvez utiliser l'option -x ou -X, mais pas les deux. Si vous n'utilisez ni l'option -x, ni l'option -X, <i>pmrep</i> vous demande une confirmation du mot de passe.
-f	-	Facultatif. Supprime un référentiel global et désinscrit les référentiels locaux. Tous les référentiels locaux enregistrés doivent être en cours d'exécution.

DeleteConnection

Supprime une connexion relationnelle depuis le référentiel.

La commande DeleteConnection utilise la syntaxe suivante :

```
deleteconnection  
  
-n <connection_name>  
  
[-f (force delete)]  
  
[-s <connection type application, relational, ftp, loader or queue>]
```

Le tableau suivant décrit les options et arguments de *pmrep DeleteConnection* :

Option	Argument	Description
-n	connection_name	Obligatoire. Nom de la connexion à supprimer.
-f	-	Facultatif. La connexion sera supprimée sans aucune autre confirmation.
-s	type de connexion application, relationnel, ftp, chargement ou file d'attente	Facultatif. Type de connexion. Une connexion peut avoir l'un des types suivants : <ul style="list-style-type: none">- Application- FTP- Chargeur- File d'attente- Relationnel La valeur par défaut est Relationnel.

DeleteDeploymentGroup

Supprime un groupe de déploiement. Si vous supprimez un groupe de déploiement statique, vous supprimez également tous les objets du groupe de déploiement.

La commande DeleteDeploymentGroup utilise la syntaxe suivante :

```
deletedeploymentgroup  
-p <deployment_group_name>  
[-f (force delete)]
```

Le tableau suivant décrit les options et arguments de *pmrep* DeleteDeploymentGroup :

Option	Argument	Description
-p	deployment_group_name	Obligatoire. Nom du groupe de déploiement à supprimer.
-f	-	Facultatif. Supprime le groupe de déploiement sans confirmation. Si vous omettez cet argument, <i>pmrep</i> vous demande confirmation avant de supprimer le groupe de déploiement.

DeleteFolder

Supprime un dossier du référentiel.

La commande DeleteFolder utilise la syntaxe suivante :

```
deletefolder  
-n <folder_name>
```

Le tableau suivant décrit les options et arguments de *pmrep* DeleteFolder :

Option	Argument	Description
-n	folder_name	Obligatoire. Nom du dossier.

DeleteLabel

Supprime un libellé et retire le libellé de tous les objets qui l'utilisent. Si le libellé est verrouillé, la suppression échoue.

La commande DeleteLabel utilise la syntaxe suivante :

```
deletelabel  
-a <label_name>  
[-f (force delete)]
```

Le tableau suivant décrit les options et arguments de *pmrep DeleteLabel* :

Option	Argument	Description
-a	label_name	Obligatoire. Nom du libellé à supprimer.
-f	-	Facultatif. Supprime le libellé sans confirmation. Si vous omettez cet argument, la commande vous demande confirmation avant d'effacer le libellé.

DeleteObject

Supprime un objet. Utilisez DeleteObject pour supprimer une source, une cible, une fonction définie par l'utilisateur, un mapplet, un mappage, une session, un worklet ou un flux de travail.

La commande DeleteObject utilise la syntaxe suivante :

```
DeleteObject  
-o <object_type>  
-f <folder_name>  
-n <object_name>  
[-s dbd_separator]
```

Le tableau suivant décrit les options et arguments de *pmrep DeleteObject* :

Option	Argument	Description
-o	object_type	Type obligatoire de l'objet que vous supprimez : source, cible, mapplet, mappage, session, fonction définie par l'utilisateur, worklet, flux de travail.
-f	folder_name	Nom obligatoire du dossier qui contient l'objet.
-n	object_name	Obligatoire. Nom de l'objet que vous supprimez. Si vous supprimez une définition source, vous devez y ajouter le nom de la base de données. Par exemple, DBD.sourcename.
-s	dbd_separator	Facultatif. Si une source ODBC comporte un point (.) dans le nom, définissez un autre caractère de séparation lorsque vous définissez l'objet source. Par exemple, au lieu de database_name.source_name, définissez l'objet source comme database_name\source_name et définissez dbd_separator comme une barre oblique inversée (\).

Remarque: Vous pouvez exécuter la commande DeleteObject sur un référentiel sans version. Si vous exécutez la commande DeleteObject sur un référentiel avec version, *pmrep* renvoie l'erreur suivante :

```
This command is not supported because the versioning is on for the repository  
<Repository name>.  
Failed to execute DeleteObject
```

DeleteQuery

Supprime une demande d'objet du référentiel. Vous ne pouvez pas supprimer une demande d'objet associée à un groupe de déploiement.

La commande DeleteQuery utilise la syntaxe suivante :

```
deletequery
-n <query_name>
-t <query_type (shared or personal)>
[-f (force delete)]
```

Le tableau suivant décrit les options et arguments de la commande *pmrep* DeleteQuery :

Option	Argument	Description
-n	query_name	Requis. Nom de la requête à supprimer.
-t	query_type	Requis. Type de requête. Vous pouvez spécifier shared ou personal.
-f	-	Facultatif. Supprime la requête sans confirmation. Si vous omettez cet argument, la commande vous demande confirmation avant de supprimer la requête.

DeployDeploymentGroup

Déploie un groupe de déploiement. Vous pouvez utiliser cette commande pour copier un groupe de déploiement dans un référentiel ou dans un autre référentiel.

Pour utiliser cette commande, vous devez créer un fichier de contrôle avec toutes les spécifications obligatoires par l'assistant Copy. Le fichier de contrôle est un fichier XML défini par le fichier depcntl.dtd.

Si *pmrep* ne peut pas immédiatement acquérir les verrous d'objet dans le référentiel cible, la commande attendra par défaut indéfiniment l'acquisition des verrous.

Vous pouvez utiliser les paramètres du fichier de contrôle de déploiement pour spécifier un dépassement de délai de déploiement. Le dépassement de délai de déploiement est le temps (en secondes) passé par *pmrep* à attendre l'acquisition des verrous. Une valeur 0 fait échouer le déploiement si *pmrep* n'arrive pas à acquérir immédiatement les verrous. La valeur par défaut est -1, qui demande à *pmrep* d'attendre indéfiniment l'acquisition des verrous.

Appuyez sur CTRL+C pour annuler le déploiement pendant l'opération de déploiement ou pendant que *pmrep* attend l'acquisition des verrous d'objet.

La commande DeployDeploymentGroup utilise la syntaxe suivante :

```
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>]

```

Le tableau suivant décrit les options et arguments de *pmrep* DeployDeploymentGroup :

Option	Argument	Description
-p	deployment_group_name	Obligatoire. Nom du groupe à déployer.
-c	control_file_name	Obligatoire. Nom du fichier XML contenant les spécifications de l'assistant Copy. Le fichier de contrôle de déploiement est obligatoire.
-r	target_repository_name	Obligatoire. Nom du référentiel cible où vous copiez le groupe de déploiement.
-n	target_repository_user_name	Obligatoire si vous copiez le groupe de déploiement vers un autre référentiel. Nom d'utilisateur de connexion au référentiel cible.
-s	target_repository_user_security_domain	Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. La valeur par défaut est Natif.
-x	target_repository_password	Facultatif. Mot de passe de connexion au référentiel cible. Vous utilisez l'option -x ou -X, mais pas les deux. Si vous copiez le groupe de déploiement vers un autre référentiel et que vous n'utilisez pas l'option -x ou -X, <i>pmrep</i> vous demande le mot de passe.
-X	target_repository_password_environment_variable	Facultatif. Variable d'environnement de mot de passe de connexion au référentiel cible. Vous utilisez l'option -x ou -X, mais pas les deux. Si vous copiez le groupe de déploiement vers un autre référentiel et que vous n'utilisez pas l'option -x ou -X, <i>pmrep</i> vous demande le mot de passe.
-d	target_domain_name	Obligatoire si vous copiez le groupe de déploiement vers un autre référentiel et que vous n'utilisez pas les options -h et -o. Nom de domaine du référentiel.
-h	target_portal_host_name	Obligatoire si vous copiez le groupe de déploiement vers un autre référentiel et que vous n'utilisez pas l'option -d. Nom de la machine du nœud qui héberge le domaine du référentiel cible.
-o	target_portal_port_number	Obligatoire si vous copiez le groupe de déploiement vers un autre référentiel et que vous n'utilisez pas l'option -d. Numéro de port du nœud qui héberge le domaine du référentiel cible.
-l	log_file_name	Facultatif. Fichier journal qui enregistre chaque étape du déploiement. Si vous omettez cette option, <i>pmrep</i> affiche les étapes du déploiement dans la fenêtre de ligne de commande.

DeployFolder

Déploie un dossier. Vous pouvez utiliser cette commande pour copier un dossier dans un référentiel ou dans un autre référentiel.

Pour utiliser cette commande, vous devez créer un fichier de contrôle avec toutes les spécifications obligatoires par l'assistant Copy. Le fichier de contrôle est un fichier XML défini par le fichier depcntl.dtd.

Si *pmrep* ne peut pas immédiatement acquérir les verrous d'objet dans le référentiel cible, la commande attendra par défaut indéfiniment l'acquisition des verrous.

Vous pouvez utiliser les paramètres du fichier de contrôle de déploiement pour spécifier un dépassement de délai de déploiement. Le dépassement de délai de déploiement est le temps (en secondes) passé par *pmrep* à attendre l'acquisition des verrous. Une valeur 0 fait échouer le déploiement si *pmrep* n'arrive pas à acquérir immédiatement les verrous. La valeur par défaut est -1, qui demande à *pmrep* d'attendre indéfiniment l'acquisition des verrous.

Appuyez sur CTRL+C pour annuler le déploiement pendant l'opération de déploiement ou pendant que *pmrep* attend l'acquisition des verrous d'objet.

La commande DeployFolder utilise la syntaxe suivante :

```
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>]
```

Le tableau suivant décrit les options et arguments de *pmrep* DeployFolder :

Option	Argument	Description
-f	folder_name	Obligatoire. Nom du dossier à déployer.
-c	control_file_name	Obligatoire. Nom du fichier XML contenant les spécifications de l'assistant Copy.
-r	target_repository_name	Obligatoire. Nom du référentiel cible dans lequel vous copiez le dossier.
-n	target_repository_user_name	Obligatoire si vous copiez le dossier dans un autre référentiel. Nom d'utilisateur de connexion au référentiel cible.

Option	Argument	Description
-s	target_repository_user_ security_domain	Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. La valeur par défaut est Natif.
-x	target_repository_user_ mot de passe	Facultatif. Mot de passe de connexion au référentiel cible. Utilisez l'option -x ou -X, mais pas les deux. Si vous copiez le dossier dans un autre référentiel et que vous n'utilisez pas l'option -x ou -X, <i>pmrep</i> vous demande le mot de passe.
-X	target_repository_password_ environment_variable	Facultatif. Variable d'environnement de mot de passe de connexion au référentiel cible. Utilisez l'option -x ou -X, mais pas les deux. Si vous copiez le dossier dans un autre référentiel et que vous n'utilisez pas l'option -x ou -X, <i>pmrep</i> vous demande le mot de passe.
-d	target_domain_name	Obligatoire si vous copiez le dossier dans un autre référentiel et que vous n'utilisez pas les options -h et -o. Nom du domaine pour le référentiel.
-h	target_portal_host_name	Obligatoire si vous copiez le dossier dans un autre référentiel et que vous n'utilisez pas l'option -d. Nom de la machine du nœud qui héberge le domaine du référentiel cible.
-o	target_portal_port_number	Obligatoire si vous copiez le dossier dans un autre référentiel et que vous n'utilisez pas l'option -d. Numéro de port du nœud qui héberge le domaine du référentiel cible.
-l	log_file_name	Facultatif. Fichier journal qui enregistre chaque étape du déploiement. Si vous omettez cette option, <i>pmrep</i> affiche les étapes du déploiement dans la fenêtre de ligne de commande.

ExecuteQuery

Exécute une requête. Vous pouvez choisir d'afficher le résultat ou d'écrire le résultat dans un fichier d'entrée persistant. Si la requête est réussie, cela renvoie le nombre total d'enregistrements éligibles.

Utilisez le fichier d'entrée persistant avec les commandes ApplyLabel, AddToDeploymentGroup, MassUpdate et Validate.

La commande ExecuteQuery utilise la syntaxe suivante :

```
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>]

```

Le tableau suivant décrit les options et arguments de *pmrep* ExecuteQuery :

Option	Argument	Description
-q	query_name	Obligatoire. Nom de la requête à exécuter.
-t	query_type	Facultatif. Type de requête à exécuter. Vous pouvez spécifier public ou private. Si non spécifié, <i>pmrep</i> recherche d'abord le nom de requête correspondant dans toutes les requêtes privées. Ensuite, la commande recherche dans les requêtes publiques.
-u	persistent_output_file_name	Facultatif. Envoyer le résultat de la requête vers un fichier texte. Si vous n'entrez pas un nom de fichier, le résultat de la requête est envoyé à stdout.
-a	-	Facultatif. Ajoute les résultats de la requête au fichier de sortie persistant. Si vous n'entrez pas cette option, <i>pmrep</i> écrase le contenu du fichier.
-c	column_separator	Facultatif. Caractère ou jeu de caractères utilisé pour séparer les colonnes des métadonnées de l'objet. Utilisez un caractère ou un jeu de caractères qui n'est pas utilisé dans les noms d'objets du référentiel. Si un des noms d'objets du référentiel contient des espaces, vous ne devriez pas utiliser d'espace comme séparateur de colonne. Si vous omettez cette option, <i>pmrep</i> utilise un espace unique.
-r	end-of-record_separator	Facultatif. Caractère ou jeu de caractères utilisé pour spécifier la fin des métadonnées de l'objet. Utilisez un caractère ou un jeu de caractères qui n'est pas utilisé dans les noms d'objets du référentiel. Si vous omettez cette option, <i>pmrep</i> utilise une nouvelle ligne.
-l	end-of-listing_indicator	Facultatif. Caractère ou jeu de caractères utilisé pour spécifier la fin de la liste d'objet. Entrez un caractère ou un jeu de caractères qui n'est pas utilisé dans les noms d'objets du référentiel. Si vous omettez cette option, <i>pmrep</i> utilise un point.
-b	-	Facultatif. Commentaires prolixes. Affiche d'autres informations en plus des informations minimales sur les objets. Si vous omettez cette option, <i>pmrep</i> imprime un format plus court comprenant le type d'objet, le mot reusable ou non-reusable, le nom de l'objet et son chemin. Le format prolix inclut le statut de l'objet, le numéro de version, le nom de dossier et les informations extraites. Le format court pour les objets globaux, comme le libellé, la requête, le groupe de déploiement et la connexion inclut le type et le nom de l'objet. Le format prolix inclut le type de libellé, le type de requête, le type de groupe de déploiement, le nom du créateur et l'heure de création.
-y	-	Facultatif. Affiche le type de base de données des sources et des cibles.

Option	Argument	Description
-n	-	Facultatif. N'inclut pas le chemin parent complet des objets non réutilisables dans le résultat de requête. Par exemple, si vous utilisez cette option et que le résultat inclut une transformation non réutilisable, <i>pmrep</i> imprime transformation_name au lieu de mapping_name.transformation_name. Cette option peut améliorer les performances de <i>pmrep</i> .
-s	dbd_separator	Facultatif. Si une source ODBC comporte un point (.) dans le nom, définissez un autre caractère de séparation lorsque vous définissez l'objet source. Par exemple, au lieu de database_name.source_name, définissez l'objet source comme database_name\source_name et définissez dbd_separator comme une barre oblique inversée (\).

Exit

Quitte le mode interactif de *pmrep*.

Le mode ligne de commande appelle et quitte *pmrep* à chaque fois que vous exécutez une commande.

La commande Exit utilise la syntaxe suivante :

```
exit
```

FindCheckout

Affiche une liste des objets extraits dans le référentiel. La liste contient les éléments extraits sauf si vous entrez « all users ».

Si vous choisissez un type d'objet, vous pouvez lister les objets extraits dans un dossier spécifique ou dans tous les dossiers. Si vous ne spécifiez pas un type d'objet, *pmrep* renvoie tous les objets extraits du référentiel.

La commande FindCheckout utilise la syntaxe suivante :

```
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>]
```

Le tableau suivant décrit les options et arguments de *pmrep* FindCheckout :

Option	Argument	Description
-o	object_type	Type d'objet que vous voulez lister. Vous pouvez spécifier la source, la cible, la transformation, le mappage, la session, le worklet, le flux de travail, le planificateur, la configuration de session, la tâche, le cube ou la dimension. Si vous n'utilisez pas cette option, <i>pmrep</i> ignore les options -f et -u et la commande renvoie tous les objets extraits du référentiel.
-f	folder_name	Facultatif si vous spécifiez un type d'objet. Renvoie une liste des objets extraits pour le type d'objet dans le dossier spécifié. Par défaut, la commande liste les objets pour le type d'objet de tous les dossiers.
-u	-	Facultatif. Liste les objets extraits par tous les utilisateurs. Par défaut, la commande liste les objets extraits par l'utilisateur actuel.
-c	column_separator	Facultatif. Caractère ou jeu de caractères utilisé pour séparer les colonnes des métadonnées de l'objet. Utilisez un caractère ou un jeu de caractères qui n'est pas utilisé dans les noms d'objets du référentiel. Si un des noms d'objets du référentiel contient des espaces, vous ne devriez pas utiliser d'espace comme séparateur de colonne. Si vous omettez cette option, <i>pmrep</i> utilise un espace unique.
-r	end-of-record_separator	Facultatif. Caractère ou jeu de caractères utilisé pour spécifier la fin des métadonnées de l'objet. Utilisez un caractère ou un jeu de caractères qui n'est pas utilisé dans les noms d'objets du référentiel. La valeur par défaut est newline /n.
-l	end-of-listing_indicator	Facultatif. Caractère ou jeu de caractères utilisé pour spécifier la fin de la liste d'objet. Utilisez un caractère ou un jeu de caractères qui n'est pas utilisé dans les noms d'objets du référentiel. Si vous omettez cette option, <i>pmrep</i> utilise un point.
-b	-	Facultatif. Commentaires prolixes. Affiche d'autres informations en plus des informations minimales sur les objets. Si vous omettez cette option, <i>pmrep</i> imprime un format plus court comprenant le type d'objet, le mot reusable ou non-reusable, le nom de l'objet et son chemin. Le format prolix inclut le numéro de version et le nom du dossier. Le format court pour les objets globaux comme le libellé, la requête, le groupe de déploiement et la connexion, inclut le type et le nom de l'objet. Le format prolix inclut le nom du créateur et l'heure de création.
-y	-	Facultatif. Affiche le type de base de données des sources et des cibles.
-s	dbd_separator	Facultatif. Si une source ODBC comporte un point (.) dans le nom, définissez un autre caractère de séparation lorsque vous définissez l'objet source. Par exemple, au lieu de database_name.source_name, définissez l'objet source comme database_name\source_name et définissez dbd_separator comme une barre oblique inversée (\).

GetConnectionDetails

Répertorie les propriétés et les attributs d'un objet de connexion sous la forme de paires nom-valeur.

Pour utiliser la commande GetConnectionDetails, vous devez avoir l'autorisation de lecture sur l'objet de connexion.

La commande GetConnectionDetails utilise la syntaxe suivante :

```
getconnectiondetails  
  
-n <connection_name>  
  
-t <connection_type>
```

Le tableau suivant décrit les options et arguments de *pmrep* GetConnectionDetails :

Option	Argument	Description
-n	connection_name	Obligatoire. Nom de la connexion dont les détails sont à lister.
-t	connection_type	Obligatoire. Type de connexion. Une connexion peut avoir l'un des types suivants : <ul style="list-style-type: none">- Application- FTP- Chargeur- File d'attente- Relationnel

GenerateAbapProgramToFile

Génère le programme ABAP pour un mappage avec la table SAP comme source et enregistre le programme en tant que fichier. La commande GenerateAbapProgramToFile génère le programme ABAP pour un mappage dans le référentiel PowerCenter. Le programme généré est enregistré en tant que fichier. Vous pouvez utiliser la commande GenerateAbapProgramToFile pour les mappages qui utilisent des tables SAP comme source.

La convention de nommage pour le fichier est *nomdemappage_<version>_<mode_programme>.ab4*. Placez le chemin et le nom de fichier entre guillemets doubles. Après avoir généré et sauvegardé le programme ABAP dans un fichier, utilisez la commande InstallAbapProgram pour l'installer dans un système SAP.

La commande GenerateAbapProgramToFile utilise la syntaxe suivante :

```
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)]

```

Le tableau suivant décrit les options et arguments de pmrep GenerateAbapProgramToFile :

Option	Argument	Description
-s	folder_name	Obligatoire. Le nom du dossier qui contient le mappage pour lequel le programme ABAP doit être généré.
-m	mapping_name	Obligatoire. Nom du mappage.
-v	version_number	Facultatif. Numéro de version du mappage. La valeur par défaut est la dernière version.
-l	log_filename	Facultatif. Nom du fichier journal où les informations ou des messages d'erreur sont écrits. Par défaut, le fichier journal est créé dans le répertoire où vous exécutez la commande.
-u	user_name	Obligatoire. Nom d'utilisateur de connexion du système source SAP. Doit être un utilisateur pour lequel vous avez créé une connexion de système source.
-x	mot de passe	Obligatoire. Mot de passe pour le nom d'utilisateur. Utilisez le programme de ligne de commande pmpasswd pour crypter le mot de passe utilisateur.
-c	connect_string	Obligatoire. Entrée DEST définie dans le fichier <code>sapnwrfc.ini</code> pour une connexion à un serveur d'application SAP spécifique ou pour une connexion qui utilise l'équilibrage de charge SAP.
-t	client	Obligatoire. Numéro de client SAP.
-y	langue	Facultatif. Langue de connexion SAP. Doit être compatible avec le code page client PowerCenter. La valeur par défaut est la langue du système SAP.
-p	program_mode (file, stream)	Obligatoire. Mode dans lequel le service d'intégration PowerCenter extrait les données depuis le système SAP. Sélectionnez le fichier ou le flux.
-f	output_file_location	Obligatoire. Emplacement dans la machine locale où vous souhaitez enregistrer le fichier du programme ABAP.
-e	-	Facultatif. Écrase le nom de fichier par défaut du programme ABAP.
-o	override_name	Obligatoire si vous activez l'écrasement. Nom de fichier du programme ABAP.

Option	Argument	Description
-a	-	Facultatif. Ajoute la vérification des autorisations au programme ABAP.
-n	-	Facultatif. Ajoute un espace de nom que vous avez enregistré avec SAP au nom de programme ABAP.

Exemple

L'exemple suivant génère un programme ABAP et l'enregistre dans un fichier :

```
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"
```

Aide

Renvoie la syntaxe de commande spécifiée. Si vous ne spécifiez pas une commande, la syntaxe de toutes les commandes *pmrep* est affichée.

Pour la commande Help, utilisez l'une des structures de syntaxe suivantes :

```
help [command]
-help [command]
```

InstallAbapProgram

Installe un programme ABAP dans le système SAP. Utilisez la commande InstallAbapProgram pour générer et installer le programme ABAP directement sur le système SAP. Vous pouvez utiliser cette commande pour installer un programme ABAP depuis un fichier sur le système SAP. Vous pouvez utiliser la commande InstallAbapProgram pour les mappages qui utilisent des tables SAP comme source.

La commande InstallAbapProgram obtient les informations de mappage d'un mappage depuis le référentiel PowerCenter et génère le programme ABAP. La commande installe le programme ABAP généré dans le système SAP. La première fois que vous installez le programme ABAP sur le système SAP, la commande génère un nom de programme. Les installations suivantes utilisent le même nom de programme si vous utilisez le même mode de programme.

Lorsque vous installez un programme ABAP sur le système SAP depuis un fichier, vous devez fournir le chemin d'accès complet et le nom du fichier du programme ABAP que vous voulez installer. Vous devez placer le chemin et le nom de fichier entre guillemets doubles. Vous devez fournir le nom de dossier et les informations de mappage pour lesquels vous avez généré le programme ABAP. La commande InstallAbapProgram obtient la description du mappage et l'ajoute au programme ABAP lorsqu'il est installé sur le système SAP.

La commande InstallAbapProgram utilise la syntaxe suivante :

```
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>]

```

Le tableau suivant décrit les options et arguments de pmrep InstallAbapProgram :

Option	Argument	Description
-s	folder_name	Obligatoire. Le nom du dossier qui contient le mappage pour lequel le programme ABAP doit être généré. Si vous faites l'installation depuis un fichier, le nom du dossier qui contient le mappage pour lequel vous avez généré le programme ABAP.
-m	mapping_name	Obligatoire. Nom du mappage. Si vous faites l'installation depuis un fichier, le nom du mappage pour lequel vous avez généré le programme ABAP.
-v	version_number	Facultatif. Numéro de version du mappage. La valeur par défaut est la dernière version. Si vous faites l'installation depuis un fichier, la version du mappage pour laquelle vous avez généré le programme ABAP.
-l	log_filename	Facultatif. Nom du fichier journal où les informations ou des messages d'erreur sont écrits. Par défaut, le fichier journal est stocké dans le répertoire où vous exécutez la commande.
-u	user_name	Obligatoire. Nom d'utilisateur de connexion du système source SAP. Doit être un utilisateur pour lequel vous avez créé une connexion de système source.
-x	mot de passe	Obligatoire. Mot de passe pour le nom d'utilisateur. Utilisez le programme de ligne de commande pmpasswd pour crypter le mot de passe utilisateur.
-c	connect_string	Obligatoire. Entrée DEST définie dans le fichier <code>sapnwrfc.ini</code> pour une connexion à un serveur d'application SAP spécifique ou pour une connexion qui utilise l'équilibrage de charge SAP.
-t	client	Obligatoire. Numéro de client SAP.
-y	langue	Facultatif. Langue de connexion SAP. Doit être compatible avec le code page client PowerCenter. La valeur par défaut est la langue du système SAP.

Option	Argument	Description
-f	input_file_name	Obligatoire si vous installez le programme ABAP depuis un fichier. Nom du fichier du programme ABAP à partir duquel vous voulez installer le programme ABAP dans le système SAP.
-p	program_mode (file, stream)	Obligatoire si vous générez et installez le programme ABAP directement sur le système SAP. Facultatif si vous installez le programme ABAP depuis un fichier. Mode dans lequel le service d'intégration PowerCenter extrait les données depuis le système SAP. Sélectionnez le fichier ou le flux.
-e	-	Facultatif si vous générez et installez le programme ABAP directement sur le système SAP. Écrase le nom de fichier par défaut du programme ABAP.
-o	override_name	Obligatoire si vous activez l'écrasement. Nom de fichier du programme ABAP.
-a	-	Facultatif si vous générez et installez le programme ABAP directement sur le système SAP. Ajoute la vérification des autorisations au programme ABAP.
-n	-	Facultatif si vous générez et installez le programme ABAP directement sur le système SAP. Ajoute un espace de nom que vous avez enregistré avec SAP au nom de programme ABAP.
-d	development_class_name	Facultatif. Package ou nom de la classe de développement où le service de référentiel PowerCenter installe le programme ABAP. La classe de développement par défaut est \$TMP.

Exemples

L'exemple suivant installe le programme ABAP directement sur le système SAP :

```
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
```

L'exemple suivant installe le programme ABAP depuis un fichier sur le système SAP :

```
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

Arrête les connexions utilisateur au référentiel. Vous pouvez arrêter les connexions utilisateur selon le nom d'utilisateur ou l'identifiant de connexion. Vous pouvez également arrêter toutes les connexions utilisateur au référentiel.

La commande DétruireConnexionUtilisateur utilise la syntaxe suivante :

```
killuserconnection
{-i <connection_id> |
-n <user_name> |
-a (kill all)}
```

Le tableau suivant décrit les options et arguments de *pmrep* DétruireConnexionUtilisateur :

Option	Argument	Description
-i	connection_id	Identifiant de connexion du référentiel.
-n	user_name	Nom d'utilisateur.
-a	-	Arrête toutes les connexions.

ListConnections

Répertorie tous les objets de connexion du référentiel et leurs types de connexion respectifs. Les types de connexion sont les suivants :

- Application
- FTP
- Chargeur
- File d'attente
- Relationnel

La commande ListConnections utilise la syntaxe suivante :

```
listconnections  
[-t (output includes connection subtype)]
```

Le tableau suivant décrit l'option *pmrep* ListConnections :

Option	Argument	Description
-t	-	Facultatif. Affiche le sous-type de connexion. Par exemple, pour une connexion relationnelle, les sous-types de connexion comprennent Oracle, Sybase et Microsoft SQL Server. Vous pouvez uniquement afficher le sous-type des connexions pour lesquelles vous avez l'autorisation d'accès en lecture.

Pour plus d'informations sur les sous-types de connexion, consultez ["Sous-types de connexion" à la page 1384](#).

ListObjectDependencies

Répertorie les objets de dépendances des objets réutilisables et non réutilisables. Si vous voulez lister les dépendances des objets non réutilisables, vous devez utiliser un fichier d'entrée persistant contenant les identifiants des objets. Vous pouvez créer ce fichier par l'exécution d'une requête et par la création d'un fichier texte.

ListObjectDependencies accepte un fichier d'entrée persistant et peut créer un fichier de sortie persistant. Ces fichiers sont au même format. Si vous créez un fichier de sortie, utilisez-le comme entrée dans les commandes *pmrep* ApplyLabel, AddToDeployment Group ou Validate.

ListObjectDependencies renvoie le nombre d'enregistrements si la commande fonctionne correctement.

La commande ListObjectDependencies utilise la syntaxe suivante :

```
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>]
```

Le tableau suivant décrit les options et arguments de *pmrep* ListObjectDependencies :

Option	Argument	Description
-n	object_name	Requis. Nom d'un objet spécifique dont les dépendances sont à lister.
-o	object_type	Requis. Type de l'objet dont les dépendances sont à lister. Vous pouvez spécifier la source, la cible, la transformation, le mappage, la session, le worklet, le flux de travail, le planificateur, la session, la configuration de session, la tâche, le cube, la dimension, la requête et le groupe de déploiement.
-t	object_subtype	Type de transformation, de tâche ou de requête. Ignoré pour d'autres types d'objets. Pour plus d'informations sur les sous-types valides, consultez "Liste des types d'objets" à la page 1433 .
-v	version_number	Facultatif. Liste les objets dépendants pour une version d'objet autre que la dernière version. Vous devez utiliser cette option uniquement pour les référentiels avec version. Cela ne s'applique pas aux référentiels sans version.
-f	folder_name	Dossier contenant le nom d'objet. Le dossier est requis si vous n'utilisez pas l'option -i.

Option	Argument	Description
-i	persistent_input_file	Facultatif. Fichier texte d'objets générés à partir des commandes ExecuteQuery ou Validate. Vous devez utiliser ce fichier si vous voulez lister les dépendances pour les objets non réutilisables. Si vous utilisez cette option, vous ne pouvez pas utiliser les options -n, -o, -f pour spécifier les objets.
-d	dependency_object_types	Facultatif. Type d'objets dépendants à lister. Vous pouvez entrer ALL ou bien un ou plusieurs types d'objets. La valeur par défaut est ALL. Si ALL, <i>pmrep</i> liste tous les objets dépendants pris en charge. Si vous choisissez un ou plusieurs objets, <i>pmrep</i> liste les objets dépendants de ces types. Pour entrer plusieurs types d'objets, séparez-les par des virgules sans espace.
-p	dependency_direction	Requis si vous n'utilisez pas l'option -s. Les objets dépendants parents ou enfants à lister. Vous pouvez spécifier des parents, des enfants ou les deux. Si vous n'utilisez pas l'option -p, <i>pmrep</i> ne répertorie pas les dépendances parents ou enfants.
-s	-	Requis si vous n'utilisez pas l'option -p. Inclure l'objet de dépendance clé primaire et clé étrangère indépendamment de la direction de la dépendance. Si vous n'utilisez pas l'option -s, <i>pmrep</i> ne répertorie pas les dépendances de clé primaire/clé étrangère.
-g	-	Facultatif. Trouver les dépendances des objets entre les référentiels.
-u	persistent_output_file_name	Envoyez le résultat des dépendances dans un fichier texte. Utilisez le fichier texte comme entrée dans les commandes <i>pmrep</i> ApplyLabel, AddToDeployment Group ou Validate. La valeur par défaut envoie le résultat de la requête vers stdout. Vous ne pouvez pas utiliser les options -b et -c avec cette option.
-a	-	Adjoindre le résultat au fichier de sortie persistant au lieu de l'écraser.
-c	column_separator	Caractère ou jeu de caractères utilisé pour séparer les colonnes des métadonnées de l'objet. Utilisez un caractère ou un ensemble de caractères non utilisé dans les noms d'objets du référentiel. Si un des noms d'objets du référentiel contient des espaces, vous ne devriez pas utiliser d'espace comme séparateur de colonne. Vous ne pouvez pas utiliser cette option avec l'option -u. Si vous omettez cette option, la commande <i>pmrep</i> utilise une espace unique.
-r	end-of-record_separator	Caractère ou jeu de caractères utilisé pour spécifier la fin des métadonnées de l'objet. Utilisez un caractère ou un ensemble de caractères non utilisé dans les noms d'objets du référentiel. La valeur par défaut est newline /n.
-l	end-of-listing_indicator	Caractère ou ensemble de caractères utilisé pour spécifier la fin de la liste d'objet. Entrez un caractère ou un ensemble de caractères non utilisé dans les noms d'objets du référentiel. Si vous omettez cette option, la commande <i>pmrep</i> utilise un point.

Option	Argument	Description
-b	-	Commentaires. Affiche d'autres informations en plus des informations minimales sur les objets. Si vous omettez cette option, la commande <i>pmrep</i> affiche un format plus court comprenant le type d'objet, le mot réutilisable ou non réutilisable, le nom de l'objet et son chemin. Le format des commentaires inclut le numéro de version et le nom du dossier. Le format court pour les objets globaux, comme le libellé, la requête, le groupe de déploiement et la connexion inclut le type et le nom de l'objet. Le format prolixe inclut le nom du créateur et l'heure de création. Vous ne pouvez pas utiliser cette option avec l'option -u.
-y	-	Facultatif. Affiche le type de base de données des sources et des cibles.
-e	dbd_separator	Facultatif. Si une source ODBC comporte un point (.) dans le nom, définissez un autre caractère de séparation lorsque vous définissez l'objet source. Par exemple, au lieu de database_name.source_name, définissez l'objet source en tant que database_name\source_name et dbd_separator en tant que barre oblique inversée (\).

ListObjects

Renvoie une liste des objets du référentiel. Lorsque vous répertoriez les objets, *pmrep* renvoie les métadonnées d'objet. Utilisez les opérations de liste suivantes :

- **Lister les types d'objets.** Définissez les objets que vous voulez lister.
- **Lister les dossiers.** Lister tous les dossiers du référentiel.
- **Lister les objets.** Lister les objets réutilisables et non réutilisables du référentiel ou d'un dossier.

Utilisez ListObjects dans un script shell pour renvoyer les métadonnées de l'objet, analyser les métadonnées, puis utiliser les données analysées dans une autre commande *pmrep*.

Par exemple, utilisez ListObjects pour créer la liste de toutes les transformations Générateur de séquence dans le référentiel. Créez un script shell qui utilise ListObjects pour renvoyer les informations de transformation Générateur de séquence, analyser les données ListObjects renvoyées et utiliser UpdateSeqGenVals pour mettre à jour les valeurs de séquence.

pmrep renvoie chaque objet dans un enregistrement et renvoie les métadonnées de chaque objet dans une colonne. Par défaut, la séparation des enregistrements se fait avec une nouvelle ligne. Vous pouvez entrer les caractères à utiliser pour séparer les enregistrements et les colonnes. Vous pouvez également saisir les caractères d'indication de la fin de la liste.

Astuce: Lorsque vous entrez des caractères de séparation des enregistrements et des colonnes et d'indication de fin de liste, utilisez des caractères qui ne sont pas utilisés dans les noms des objets du référentiel. Ceci vous aide à utiliser un script shell pour analyser les métadonnées de l'objet.

La syntaxe de la commande ListObjects est la suivante :

```
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>]

```

Le tableau suivant décrit les options et arguments de *pmrep* ListObjects :

Option	Argument	Description
-o	object_type	Obligatoire. Type d'objet à lister. <ul style="list-style-type: none"> - Lorsque vous entrez le dossier, vous n'avez aucune autre option à inclure. <i>pmrep</i> ignore les options -t et -f. - Lorsque vous entrez des objets autres que des dossiers, vous devez inclure l'option -f. - Lorsque vous entrez une transformation ou une tâche, vous devez inclure l'option -f et vous pouvez éventuellement inclure l'option -t. Pour plus d'informations sur les types d'objets à utiliser avec ListObjects, consultez "Liste des types d'objets" à la page 1433 .
-t	object_subtype	Facultatif. Type de transformation ou de tâche à lister. Lorsque vous entrez une transformation ou une tâche comme type d'objet, vous pouvez inclure cette option pour renvoyer un type spécifique. Pour plus d'informations sur les types d'objets à utiliser avec ListObjects, consultez "Liste des types d'objets" à la page 1433 .
-f	folder_name	Obligatoire si vous répertoriez des objets autres que les dossiers. Dossier dans lequel rechercher. Utilisez cette option pour tous les types d'objets sauf le groupe, le dossier, le libellé et la requête de déploiement.
-c	column_separator	Facultatif. Caractère ou jeu de caractères utilisé pour séparer les colonnes des métadonnées de l'objet. Utilisez un caractère ou un ensemble de caractères non utilisé dans les noms d'objets du référentiel. Si l'un des noms d'objets du référentiel contient des espaces, évitez d'utiliser des espaces pour séparer les colonnes. Si vous omettez cette option, la commande <i>pmrep</i> utilise une espace unique.
-r	end-of-record_indicator	Facultatif. Caractère ou jeu de caractères utilisé pour spécifier la fin des métadonnées de l'objet. Utilisez un caractère ou un ensemble de caractères non utilisé dans les noms d'objets du référentiel. La valeur par défaut est newline /n.
-l	end_of_listing_indicator	Facultatif. Caractère ou ensemble de caractères utilisé pour spécifier la fin de la liste d'objet. Entrez un caractère ou un ensemble de caractères non utilisé dans les noms d'objets du référentiel. Si vous omettez cette option, la commande <i>pmrep</i> utilise un point.

Option	Argument	Description
-b	-	Facultatif. Commentaires. Affichez plus d'informations en supplément des informations minimum sur les objets. Si vous omettez cette option, vous affichez un format plus court comprenant le type d'objet, le mot reusable ou non-reusable, le nom de l'objet et son chemin. Le format prolixe inclut le statut de l'objet, le numéro de la version et les informations extraites. Le format court pour les objets globaux, comme le libellé, la requête, le groupe de déploiement et la connexion inclut le type et le nom de l'objet. Le format prolixe inclut le type de libellé, le type de requête, le type de groupe de déploiement, le nom du créateur et l'heure de création.
-y	-	Facultatif. Affiche le type de base de données des sources et des cibles.
-s	dbd_separator	Facultatif. Si une source ODBC comporte un point (.) dans le nom, définissez un autre caractère de séparation lorsque vous définissez l'objet source. Par exemple, au lieu de database_name.source_name, définissez l'objet source en tant que database_name\source_name et dbd_separator en tant que barre oblique inversée (\).

Liste des types d'objets

Utilisez l'option `object_type` pour définir les objets que vous voulez lister. La commande répertorie les dernières versions ou les versions extraites des objets, comprenant les raccourcis, mais excluant des objets selon les règles pour les types d'objets.

Le tableau suivant décrit les types d'objets et les règles que vous utilisez avec `ListObjects` :

Type d'objet	Règle
Deploymentgroup	Lister les groupes de déploiement dans le référentiel.
Dossier	Lister les dossiers dans le référentiel.
Label	Lister les libellés dans le référentiel.
Mapplet	Lister les mapplets avec la dernière version ou la version extraite dans un dossier, comprenant les raccourcis, mais excluant les instances de mapplets réutilisables.
Mappage	Lister les mappages avec la dernière version ou la version extraite dans un dossier, comprenant les raccourcis, mais excluant les instances de mapplets réutilisables.
Requête	Lister les requêtes dans le référentiel.
Planificateur	Lister les planificateurs réutilisables et non réutilisables avec la dernière version ou la version extraite dans un dossier.
Session	Lister les sessions réutilisables et non réutilisables avec la dernière version ou la version extraite dans un dossier, sauf les instances de sessions réutilisables.
Sessionconfig	Lister les configurations de session avec la dernière version ou la version extraite dans un dossier.
Source	Lister les sources avec la dernière version ou la version extraite dans un dossier, comprenant les raccourcis, mais excluant les instances de source.

Type d'objet	Règle
Cible	Lister les cibles avec la dernière version ou la version extraite dans un dossier, comprenant les raccourcis, mais excluant les instances cibles.
Tâche	Lister les tâches réutilisables et non réutilisables avec la dernière version ou la version extraite dans un dossier.
Transformation	Lister les transformations réutilisables et non réutilisables avec la dernière version ou la version extraite dans un dossier, comprenant les raccourcis et excluant les instances de transformations réutilisables.
« Fonction définie par l'utilisateur »	Lister les fonctions définies par l'utilisateur dans le référentiel.
Flux de travail	Lister les flux de travail avec la dernière version ou la version extraite dans un dossier.
Worklet	Lister les worklets réutilisables et non réutilisables et avec la dernière version ou la version extraite dans un dossier, sauf les instances de worklets réutilisables.

Le tableau suivant décrit les types d'objets et les valeurs à utiliser avec les commandes *pmrep* :

Type d'objet	Valeur de sous-type	Description
Requête	personnel	Personnel
Requête	partagé	Partagé
Tâche	attribution	Attribution
Tâche	commande	Commande
Tâche	contrôle	Contrôle
Tâche	décision	Décision
Tâche	e-mail	E-mail
Tâche	event_raise	Event raise
Tâche	event_wait	Event wait
Tâche	début	Début
Tâche	minuteur	Minuteur
Transformation	agrégation	Agrégation
Transformation	application_source_qualifier	Qualificateur source d'application
Transformation	app_multi-group_source_qualifier	Qualificateur source d'applications multigroupe
Transformation	custom_transformation	Personnalisation

Type d'objet	Valeur de sous-type	Description
Transformation	custom_transformation	HTTP
Transformation	custom_transformation	SQL
Transformation	custom_transformation	Union
Transformation	custom_transformation	Générateur XML
Transformation	custom_transformation	Analyseur XML
Transformation	expression	Expression
Transformation	external_procedure	Procédure externe
Transformation	filtre	Filtre
Transformation	input_transformation	Entrée
Transformation	java	Java
Transformation	jointure	Jointure
Transformation	lookup_procedure	Recherche
Transformation	mq_source_qualifier	Qualificateur source MQ
Transformation	normalisateur	Normalisateur
Transformation	output_transformation	Sortie
Transformation	rang	Rang
Transformation	routeur	Routeur
Transformation	séquence	Générateur de séquence
Transformation	trieur	Trieur
Transformation	source_qualifier	Qualificateur source
Transformation	stored_procedure	Procédure stockée
Transformation	transaction_control	Contrôle de transaction
Transformation	update_strategy	Stratégie de mise à jour
Transformation	xml_source_qualifier	Qualificateur source XML

Liste des dossiers

Utilisez ListObjects pour renvoyer chaque dossier du référentiel. Lorsque vous entrez `dossier` pour le type d'objet, *pmrep* ignore le sous-type et le nom de dossier.

Par exemple, pour créer la liste de tous les dossiers du référentiel, utilisez la syntaxe suivante :

```
listobjects -o folder
```

Alternativement, vous pouvez entrer un séparateur de colonne et un indicateur de fin de liste différents :

```
ListObjects -o folder -c "*" -l #
```

Liste des objets

Utilisez ListObjects pour lister les objets réutilisables et non réutilisables du référentiel ou d'un dossier.

pmrep n'inclut pas d'instances d'objets réutilisables. Lorsque vous listez des objets, vous devez inclure le nom de dossier pour tous les objets associés à un dossier.

pmrep renvoie le nom de l'objet avec le chemin le cas échéant. Par exemple, lorsqu'une transformation se trouve dans un mappage ou un mapplet, *pmrep* renvoie *mapping_name.transformation_name* ou *mapplet_name.transformation_name*.

Pour plus d'informations sur une liste des valeurs de retour de tâche ou de transformation, consultez ["Liste des types d'objets" à la page 1433](#).

Par exemple, pour créer la liste de tous les types de transformation dans un dossier, entrez le texte suivant à l'invite :

```
listobjects -o transformation -f myfolder
```

pmrep renvoie les informations suivantes :

```
stored_procedure reusable sp_sprocl
expression reusable expl
stored_procedure non-reusable mapping1.sp_nsproc
sequence non-reusable smallmapplet.seqgen_empid
.listobjects completed successfully.
```

Pour créer la liste de toutes les transformations de procédure stockée dans un dossier, entrez le texte suivant à l'invite :

```
listobjects -o transformation -t stored_procedure -f myfolder
```

pmrep renvoie les informations suivantes :

```
stored_procedure reusable sp_sprocl
stored_procedure non-reusable mapping1.sp_nsproc
.listobjects completed successfully.
```

Pour créer la liste de toutes les sessions dans un dossier, entrez le texte suivant à l'invite :

```
listobjects -o session -f myfolder
```

pmrep renvoie les informations suivantes :

```
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

Renvoie une liste de sources ou cibles utilisées dans une session. Lorsque vous listez des sources ou des cibles, *pmrep* renvoie des noms d'instances de source ou de cible à la fenêtre. Utilisez ListTablesBySess dans un script shell avec d'autres commandes *pmrep*. Par exemple, vous pouvez créer un script shell qui utilise ListTablesBySess pour renvoyer les noms d'instances de sources et utilise les noms Updatesrcprefix pour mettre à jour le nom du propriétaire de la source.

Lorsque vous utilisez `ListTablesBySess`, *pmrep* renvoie des noms d'instance de source ou de cible au fur et à mesure qu'ils apparaissent dans les propriétés de session. Par exemple, si le mappage contient un mapplet avec une source, *pmrep* renvoie le nom d'instance de source au format suivant :

```
mapplet_name.source_name
```

La commande `ListTablesBySess` utilise la syntaxe suivante :

```
listtablesbysess
-f <folder_name>
-s [<qualifying_path>.<session_name>]
-t <object_type_listed> (source or target)
```

Le tableau suivant décrit les options et arguments de *pmrep* `ListTablesBySess` :

Option	Argument	Description
-f	folder_name	Obligatoire. Nom du dossier contenant la session.
-s	session_name	Obligatoire. Nom de la session contenant les sources ou cibles. Vous pouvez entrer un nom de session réutilisable ou non réutilisable. Cependant, vous ne pouvez pas entrer une instance de nom de session réutilisable. Pour entrer un nom de session non réutilisable dans un flux de travail, entrez le nom du flux de travail et le nom de session sous la forme <i>workflow_name.session_name</i> .
-t	object_type_listed	Obligatoire. Entrez la source pour lister les sources ou entrez la cible pour lister les cibles.

Par exemple, pour lister toutes les sources dans une session réutilisable, entrez le texte suivant à l'invite :

```
listtablesbysess -f myfolder -s s_reus_sess1 -t source
```

pmrep renvoie les informations suivantes :

```
ITEMS
mapplet1.ORDERS
Shortcut_To_ITEM_ID
listtablesbysess completed successfully.
```

Lorsque le mappage contient un mapplet avec une source, *pmrep* inclut le nom du mapplet avec la source, par exemple `mapplet1.ORDERS`.

Par exemple, vous pouvez créer la liste de toutes les cibles dans une session non réutilisable d'un flux de travail :

```
listtablesbysess -f myfolder -s wf_workkflow1.s_nrsess1 -t target
```

pmrep renvoie les informations suivantes :

```
target1_inst
ORDERS_BY_CUSTID
Shortcut_To_tgt2_inst
listtablesbysess completed successfully.
```

ListUserConnections

Répertorie les informations pour chaque utilisateur connecté au référentiel.

La commande ListUserConnections utilise la syntaxe suivante :

```
listuserconnections
```

MassUpdate

Met à jour les propriétés de session pour un ensemble de sessions qui répond aux conditions spécifiées. Vous pouvez mettre à jour toutes les sessions d'un dossier ou d'une liste de sessions. Pour mettre à jour une liste de sessions, créez un fichier d'entrée persistant. La liste peut contenir une liste des sessions ou des conditions telles qu'un modèle de nom ou une valeur de propriété. Utilisez ExecuteQuery pour générer un fichier d'entrée persistant.

Lorsque vous exécutez MassUpdate, vous pouvez afficher des informations comme le nom de dossier, le nombre de sessions correctement mises à jour ou échouées et les noms des sessions qui sont mises à jour. Vous pouvez afficher le statut de la mise à jour dans la fenêtre de ligne de commande ou dans un fichier journal généré par la commande. Vous pouvez spécifier le nom et le chemin du fichier journal lorsque vous exécutez la commande. Par défaut, le fichier journal est stocké dans le répertoire où vous exécutez la commande.

Utilisez MassUpdate pour mettre à jour une propriété de session sur plusieurs sessions quand une version de PowerCenter modifie une valeur par défaut.

Remarque: Vous ne pouvez pas mettre à jour des propriétés de session dépendantes.

Avant de mettre à jour les sessions, vous pouvez également exécuter MassUpdate en mode test pour visualiser les modifications. Pour afficher un exemple de fichier journal, consultez ["Exemple de fichier journal" à la page 1444](#).

La commande MassUpdate utilise la syntaxe suivante :

```
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>]
```

Le tableau suivant décrit les options et arguments de *pmrep* MassUpdate :

Option	Argument	Description
-t	session_property_type	Obligatoire. Type de propriété de session à mettre à jour. Les types de propriété de session suivants sont disponibles : <ul style="list-style-type: none"> - session_property - session_config_property - transformation_instance_attribute - session_instance_runtime_option
-n	session_property_name	Obligatoire. Nom de l'attribut ou de la propriété à mettre à jour.
-v	session_property_value	Obligatoire. Valeur que vous souhaitez attribuer à la propriété, suivie d'un point-virgule. Par exemple, pour attribuer une valeur à la propriété, utilisez la syntaxe suivante : -v "IgnoreNULLInExpressionComparison=Yes;" Remarque: Placez la valeur de propriété de session entre guillemets doubles.
-w	transformation_type	Obligatoire si vous mettez à jour un attribut d'instance de transformation. Type de transformation à mettre à jour. Vous pouvez mettre à jour les types de transformations suivants : agrégation, jointure, procédure de recherche, rang, trieur, définition source et définition cible.
-i	persistent_input_file	Obligatoire si vous n'utilisez pas l'option -f. Nom du fichier qui contient la liste des sessions à mettre à jour. Vous pouvez utiliser la commande <i>pmrep</i> ExecuteQuery pour exécuter une requête et générer ce fichier. MassUpdate renvoie une erreur si vous spécifiez un objet qui n'est pas une session. Vous devez utiliser l'option -i ou l'option -f, mais pas les deux.
-f	folder_name	Obligatoire si vous n'utilisez pas l'option -i. Nom du dossier. Utilisez cette option pour mettre à jour toutes les sessions d'un dossier. Vous devez utiliser l'option -i ou l'option -f, mais pas les deux.
-o	condition_operator	Obligatoire si vous utilisez condition_value. Partie de la condition qui définit l'ensemble de sessions. L'attribut d'une session ou d'une instance de session est mis à jour lorsque la condition est remplie. Vous pouvez utiliser les opérateurs de condition suivants pour mettre à jour une chaîne : equal ou unequal. Vous pouvez utiliser les opérateurs de condition suivants pour mettre à jour un entier : equal, unequal, less ou greater.
-l	condition_value	Obligatoire si vous utilisez un opérateur de condition. Partie de la condition. La condition s'affiche comme suit : <session_property_value> <condition operator> <condition_value>

Option	Argument	Description
-g	update_session_instance_flag	Obligatoire si vous mettez à jour une option d'exécution d'instance de session. Facultatif pour les types de propriété de session suivants : propriété de session, attribut de configuration de session et attribut d'instance de transformation. Met à jour les instances de session. Vous pouvez mettre à jour un attribut dans une instance de session si l'instance de session écrase l'attribut.
-m	test_mode	Facultatif. Exécute MassUpdate en mode test. Affichez les sessions qui seront affectées par la commande avant de valider les modifications. Vous pouvez voir les détails suivants dans la fenêtre de ligne de commande : <ul style="list-style-type: none"> - Nom de session - Type de la session : réutilisable ou non réutilisable - Valeur actuelle de la propriété de session - Sessions pour lesquelles l'attribut a la même valeur et qui ne sont pas affectées par la commande.
-u	output_log_file_name	Facultatif. Nom du fichier journal qui stocke le statut de la mise à jour et des informations de base sur les sessions ou les instances de session. Les valeurs d'attribut précédentes sont également écrites dans ce fichier. Si vous n'utilisez pas cette option, les détails s'affichent dans la fenêtre de ligne de commande.

La commande MassUpdate renvoie « commande MassUpdate correctement terminée » ou renvoie le message « impossible d'exécuter la commande MassUpdate ». La mise à jour peut échouer pour les raisons suivantes :

- Vous n'avez pas spécifié une valeur d'attribut valide concernant le nom de l'attribut.
- Vous avez spécifié un nom de propriété de session correct avec le mauvais type de propriété de session.
- Vous n'avez pas spécifié l'option -v qui se termine par un point-virgule lors de la mise à jour d'une valeur de propriété de session.
- Vous n'avez pas spécifié l'option -w lors de la mise à jour d'un attribut d'instance de transformation.
- Vous n'avez pas spécifié l'option -g lors de la mise à jour d'une option d'exécution d'instance de session.
- Vous n'avez pas le rôle d'administrateur pour les services de référentiel.

Types de propriété de session

Lorsque vous exécutez MassUpdate, indiquez le type de propriété de session et son nom. Vous spécifiez les types de propriété de session suivants :

- Propriétés de session
- Attributs de configuration de session
- Attributs de l'instance de transformation
- Options d'exécution de l'instance de session

Remarque: Vous devez placer la propriété de session entre guillemets simples.

Le tableau suivant répertorie les propriétés de session que vous pouvez mettre à jour et les types de propriété de la session :

Propriété de session	Type de propriété de session
Valeur de connexion \$Source	session_property
Valeur de connexion \$Target	session_property
Ajout de pipelines simultanés pour la création du cache de recherche	session_config_property
Taille de cache pour les données de l'agrégation	transformation_instance_attribute L'argument transformation_type doit être agrégation.
Taille de cache pour l'index d'agrégation	transformation_instance_attribute L'argument transformation_type doit être agrégation.
Autorisez le refoulement par la séquence temporaire	session_property
Autorisez la vue temporaire pour le refoulement	session_property
Répertoire de cache	transformation_instance_attribute L'argument transformation_type doit être agrégation, jointure ou rang.
Fonction LOOKUP() du cache	session_config_property
Collecte des données de performance	session_property
Intervalle de validation	session_property
Type de validation	session_property
Classement de charge basé sur la contrainte	session_config_property
Propriétés personnalisées	session_config_property
Chaîne de format date/heure	session_config_property
Taille de bloc tampon par défaut	session_config_property
Désactivez cette tâche	session_instance_runtime_option
Taille du tampon DTM	session_property
Activer la précision élevée	session_property
Activez le chargement du test	session_property
Échec du parent si cette tâche ne s'exécute pas	session_instance_runtime_option
Échec du parent si cette tâche échoue	session_instance_runtime_option
L'agrégation incrémentielle	session_property

Propriété de session	Type de propriété de session
Est activé	session_config_property
Chemin de classe Java	session_property
Taille de cache pour les données de jointure	transformation_instance_attribute L'argument transformation_type doit être jointure.
Taille de cache pour l'index de jointure	transformation_instance_attribute L'argument transformation_type doit être jointure.
Longueur de tampon de la ligne séquentielle	session_config_property
Nom du répertoire de cache de recherche	transformation_instance_attribute L'argument transformation_type doit être « procédure de recherche ».
Taille de cache des données de recherche	transformation_instance_attribute L'argument transformation_type doit être « procédure de recherche ».
Taille de cache de l'index de recherche	transformation_instance_attribute L'argument transformation_type doit être « procédure de recherche ».
Mémoire maximum autorisée pour les attributs Auto Memory	session_config_property
Pourcentage maximum de la mémoire totale autorisée pour les attributs d'Auto Memory	session_config_property
En cas d'erreur avant ou après SQL	session_config_property
En cas d'erreur de la tâche de commande avant la session	session_config_property
En cas d'erreur de la procédure stockée	session_config_property
Répertoire du fichier de sortie	transformation_instance_attribute L'argument transformation_type doit être « définition cible ».
Écraser le traçage	session_config_property
Nom du fichier de paramètres	session_property
Compatibilité d'horodatage Pre 85	session_config_property
Cache de recherche pré-créé	session_config_property
Optimisation du refoulement	session_property
Taille de cache pour les données de rang	transformation_instance_attribute L'argument transformation_type doit être rang.

Propriété de session	Type de propriété de session
Taille de cache pour l'index du rang	transformation_instance_attribute L'argument transformation_type doit être rang.
Stratégie de récupération	session_property
Répertoire du fichier de rejet	transformation_instance_attribute L'argument transformation_type doit être « définition cible ».
Répéter les transactions pour les erreurs	session_property
Enregistrer le journal de session par	session_config_property
Répertoire du fichier journal session	session_property
Nouvelle tentative de la session lors de l'interblocage	session_property
Ordre de tri de la session	session_property Quand le service d'intégration est exécutée en mode Unicode, vous pouvez choisir l'ordre de tri des données dans la session. Vous pouvez configurer les valeurs suivantes pour l'ordre de tri : - 0. BINARY - 2. SPANISH - 3. TRADITIONAL_SPANISH - 4. DANISH - 5. SWEDISH - 6. FINNISH
Taille de cache du trieur	transformation_instance_attribute L'argument transformation_type doit être trieur.
Répertoire du fichier source	transformation_instance_attribute L'argument transformation_type doit être « définition source ».
Arrêter sur les erreurs	session_config_property
Traiter les lignes de source en tant que	session_property
Traiter le lien d'entrée comme AND	session_instance_runtime_option
Ecrire un fichier journal de session rétrocompatible	session_property

Règles et instructions pour MassUpdate

Utilisez les règles et directives suivantes lorsque vous exécutez MassUpdate :

- Si le nœud exécutant le processus de service de référentiel a une mémoire limitée, désactivez la mise en cache d'agent de référentiel avant d'exécuter MassUpdate ou redémarrez le service de référentiel après avoir exécuté MassUpdate.
- Vous pouvez mettre à jour les sessions réutilisables et les sessions non réutilisables.

- Vous pouvez mettre à jour la valeur de toute session ou de toute propriété de configuration de session prise en charge qu'elle soit ou non remplacée.
- Vous ne pouvez pas rétablir les valeurs de propriété après avoir exécuté MassUpdate.
- Vous ne pouvez pas mettre à jour les sessions qui sont extraites.
- Vous ne pouvez pas mettre à jour les sessions de dossiers gelés.

Exemple de fichier journal

Le texte suivant montre un exemple de fichier journal généré par *pmrep* MassUpdate :

```
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

Modifie les propriétés du dossier. Vous modifiez un dossier dans un référentiel sans version.

La commande renvoie « commande ModifyFolder correctement terminée » ou le message « Échec de la commande ModifyFolder ». La modification peut échouer pour les raisons suivantes :

- Le dossier n'existe pas.
- Le nouveau propriétaire n'existe pas ou n'appartient pas au groupe.
- Un dossier avec le nouveau nom de dossier existe déjà.

La commande `ModifyFolder` utilise la syntaxe suivante :

```
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>]
```

Le tableau suivant décrit les options et arguments de *pmrep ModifyFolder* :

Option	Argument	Description
-n	folder_name	Obligatoire. Nouveau nom de dossier.
-d	folder_description	Facultatif. Description du dossier qui s'affiche dans le gestionnaire du référentiel.
-o	owner_name	Facultatif. Propriétaire actuel du dossier. N'importe quel utilisateur du référentiel peut être le propriétaire du dossier. Le propriétaire par défaut est l'utilisateur actuel.
-a	owner_security_domain	Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient le propriétaire. La valeur par défaut est Natif.
-s	shared_folder	Facultatif. Partage le dossier.
-p	autorisations	Facultatif. Droits d'accès au dossier. Si omis, le service de référentiel utilise les autorisations existantes.
-r	new_folder_name	Facultatif. Nouveau nom de dossier.
-f	folder_status	Facultatif. Changer l'état du dossier dans l'un des états suivants : <ul style="list-style-type: none">- actif. Cet état permet d'extraire des objets avec version dans le dossier.- frozendeploy (Gelé, Permettre déploiement pour remplacer). Cet état empêche les utilisateurs d'archiver des objets dans le dossier. Le déploiement dans le dossier crée de nouvelles versions des objets.- frozennodeploy (Gelé, Ne pas permettre déploiement pour remplacer). Cet état empêche les utilisateurs d'archiver des objets dans le dossier. Vous ne pouvez pas déployer d'objets dans ce dossier.
-u	os_profile	Facultatif. Attribue un profil du système d'exploitation au dossier.

Notification

Envoie des messages de notification aux utilisateurs connectés à un référentiel ou aux utilisateurs connectés à tous les référentiels gérés par un service de référentiel.

La commande Notify utilise la syntaxe suivante :

```
notify
-m <message>
```

Le tableau suivant décrit les options et arguments de *pmrep* Notify :

Option	Argument	Description
-m	message	Obligatoire. Message que vous voulez envoyer.

La commande renvoie « notification correctement terminée » ou renvoie le message « impossible d'exécuter la notification ». La notification peut échouer pour les raisons suivantes :

- Le message que vous avez entré n'est pas valide.
- La connexion au service de référentiel a échoué.
- Le service de référentiel n'a pas réussi à avertir les utilisateurs.

ObjectExport

Exporte les objets dans un fichier XML défini par le fichier powrmart.dtd. Vous exportez un objet par nom. Si vous entrez un objet, vous devez entrer le nom du dossier qui le contient. Si vous n'entrez pas un numéro de version, vous exportez la dernière version de l'objet.

Utilisez un fichier d'entrée persistant pour spécifier différents objets à exporter simultanément. Vous pouvez créer ce fichier en utilisant les commandes *pmrep* ExecuteQuery, Validate ou ListObjectDependencies. Si vous utilisez le fichier d'entrée persistant, n'utilisez pas les autres paramètres pour spécifier les objets.

Si vous exportez un mappage, PowerCenter exporte par défaut le mappage et ses instances. Si vous voulez inclure les objets dépendants, vous devez ajouter l'option *pmrep* appropriée. Vous pouvez éventuellement inclure des objets dépendants réutilisables et non réutilisables, des objets référencés par des raccourcis et des objets liés par une relation de clé primaire/clé étrangère.

Pour exporter les dépendances de mappage, vous devez utiliser les options -b et -r.

La commande ObjectExport utilise la syntaxe suivante :

```
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]

```

Le tableau suivant décrit les options et arguments de *pmrep* ObjectExport :

Option	Argument	Description
-n	object_name	Obligatoire si vous n'utilisez pas l'option -i. Nom d'un objet spécifique à exporter. Si vous n'entrez pas cette option, <i>pmrep</i> exporte tous les derniers objets ou tous les objets extraits du dossier. Utilisez l'option -n ou l'option -i, mais pas les deux.
-o	object_type	Type d'objet du nom de l'objet. Vous pouvez spécifier la source, la cible, la transformation, le mappage, le mapplet, la session, le worklet, le flux de travail, le planificateur, la configuration de session ou la tâche. Si vous utilisez cette option, vous ne pouvez pas utiliser l'option -i.
-t	object_subtype	Type de transformation ou de tâche. Cet argument est ignoré pour d'autres types d'objets. Pour plus d'informations sur les sous-types valides, consultez "Liste des types d'objets" à la page 1433 .
-v	version_number	Facultatif. Exporte la version de l'objet que vous entrez.
-f	folder_name	Nom du dossier contenant l'objet à exporter. Si vous n'entrez pas un nom d'objet, <i>pmrep</i> exporte tous les objets du dossier. Si vous utilisez cette option, vous ne pouvez pas utiliser l'option -i.
-i	persistent_input_file	Obligatoire si vous n'utilisez pas l'option -n. Liste de fichiers textes d'objets générés par ExecuteQuery, Validate ou ListObjectDependencies. Il contient les enregistrements de l'objet avec les identifiants encodés. Si vous utilisez ce paramètre, vous ne pouvez pas utiliser les options -n, -o ou -f.
-m	-	Obligatoire pour exporter les objets dépendants. Exporte les définitions de la table de clé primaire lorsque vous exportez les sources et les cibles avec les clés étrangères.
-s	-	Obligatoire pour exporter les objets dépendants. Exporte l'objet d'origine référencé par le raccourci.
-b	-	Obligatoire pour exporter les objets dépendants. Exporte les objets non réutilisables utilisés par l'objet.
-r	-	Obligatoire pour exporter les objets dépendants. Exporte les objets réutilisables utilisés par l'objet.
-u	xml_output_file_name	Obligatoire. Nom du fichier XML destiné à contenir les informations de l'objet.

Option	Argument	Description
-l	log_file_name	Facultatif. Fichier journal qui enregistre chaque étape d'exportation. Si vous omettez cette option, les messages d'état s'affichent dans la fenêtre.
-e	dbd_separator	Facultatif. Si une source ODBC comporte un point (.) dans le nom, définissez un autre caractère de séparation lorsque vous définissez l'objet source. Par exemple, au lieu de database_name.source_name, définissez l'objet source comme database_name\source_name et définissez dbd_separator comme une barre oblique inversée (\).

Exemples

L'exemple suivant exporte un mappage nommé « map », localisé dans Dossier1, vers un fichier nommé map.xml :

```
objectexport -n map -o mapping -f folder1 -u map.xml
```

L'exemple suivant exporte les objets identifiés d'un fichier d'entrée persistant nommé persistent_input.xml vers un fichier nommé map.xml :

```
objectexport -i persistent_input.txt -u map.xml
```

Remarque: Si vous utilisez un fichier d'entrée persistant créé manuellement, si vous entrez « none » pour l'identifiant encodé, le message suivant s'affiche : Les identifiants ne sont pas valides. Tentative avec les noms pour [aucun,dossier1,map,mappage,aucun,1].

ObjectImport

Importe des objets depuis un fichier .xml. Cette commande requiert un fichier de contrôle pour spécifier les objets à importer et la façon de résoudre les conflits. Le fichier de contrôle est un fichier .xml défini par le fichier impcntl.dtd.

La commande ObjectImport utilise la syntaxe suivante :

```
objectimport -i <input_xml_file_name> -c <control_file_name> [-l <log_file_name>] [-p  
(conserver la valeur persistante)]
```

Le tableau suivant décrit les options et arguments de la commande *pmrep* ObjectImport :

Option	Argument	Description
-i	input_XML_file_name	Requis. Nom du fichier .xml à importer.
-c	control_file_name	Requis. Nom du fichier de contrôle qui définit les options d'importation.
-l	log_file_name	Facultatif. Fichier journal qui enregistre chaque étape d'exportation. Si vous omettez cette option, les messages d'état s'affichent dans la fenêtre.
-p	-	Facultatif. Conserve les valeurs persistantes pour les variables de mappage.

Remarque: La commande ObjectImport ne crée pas de dossier si le nom de dossier que vous entrez n'existe pas dans le référentiel.

Vous pouvez générer des journaux d'audit lorsque vous importez un fichier .xml dans le référentiel PowerCenter avec la commande pmrep ObjectImport. Lorsque vous importez un ou plusieurs objets de référentiel, vous pouvez générer des journaux d'audit. Pour inclure des pistes d'audit de sécurité dans les événements du journal d'activité utilisateur, activez la propriété SecurityAuditTrai pour le service de référentiel PowerCenter dans l'outil Administrator tool avant d'importer un fichier .xml. Les journaux d'activité utilisateur capturent tous les messages d'audit.

Les journaux d'audit contiennent les informations suivantes sur le fichier .xml importé :

- Nom d'hôte et adresse IP de l'ordinateur client à partir duquel le fichier .xml a été importé
- Chemin d'accès local complet du fichier d'importation .xml
- Nom du fichier
- Taille du fichier en octets
- Nom d'utilisateur connecté
- Nombre d'objets importés
- Horodatage de l'opération d'importation

PurgeVersion

Purge les versions d'objet depuis la base de données du référentiel. Vous pouvez purger les versions des objets supprimés et des objets actifs. Un objet est un objet supprimé si la dernière version est archivée et si l'état de la version est Deleted. D'autres objets sont des objets actifs.

Lorsque vous purgez les versions d'objets supprimés, vous purgez toutes les versions. Les objets supprimés doivent être archivés. Vous pouvez purger les versions de tous les objets supprimés ou des objets supprimés avant une heure de fin spécifique. Vous pouvez spécifier l'heure de fin comme étant une date et une heure, une date uniquement ou un nombre de jours avant la date actuelle.

Lorsque vous purgez des versions ou des objets actifs, vous pouvez spécifier des critères de purge. Vous pouvez spécifier le nombre de versions à conserver et purger les versions précédentes et vous pouvez purger les versions antérieures à une heure limite de purge. Vous ne pouvez pas purger une version extraite ou la dernière version archivée.

Si vous purgez les versions d'un objet composite, tenez compte des versions des objets dépendants qui sont purgées.

Vous pouvez utiliser l'option -k pour afficher les objets qui ne sont pas purgés et la raison pour laquelle les versions de l'objet ne sont pas purgées. Par exemple, il est possible que vous ne disposiez pas de l'autorisation de purger une version de l'objet. Vous ne pouvez pas purger les versions de l'objet qui font partie d'un groupe de déploiement.

La commande PurgeVersion utilise la syntaxe suivante :

```
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)]
```

Le tableau suivant décrit les options et arguments de *pmrep PurgeVersion* :

Option	Argument	Description
-d	all time_date num_day	Obligatoire si vous n'utilisez pas -n ou -t. Purge toutes les versions des objets archivés supprimés. Vous pouvez spécifier <code>all</code> pour tous les objets supprimés ou spécifier une heure de fin pour purger toutes les versions des objets qui ont été supprimés avant l'heure de fin. Vous spécifiez l'heure de fin au format <code>MM/DD/YYYY HH24:MI:SS</code> , au format <code>MM/DD/YYYY</code> ou sous la forme d'un nombre de jours avant la date actuelle. Si vous spécifiez un nombre de jours, la valeur doit être un entier supérieur à 0.
-n	last_n_versions_to_keep	Obligatoire si vous n'utilisez pas -d ou -t. Nombre de versions de l'objet parmi les dernières archivées à conserver comme objet actif. La valeur doit être un entier supérieur à 0. Par exemple, entrez 6 pour purger toutes les versions, sauf les six dernières archivées. Si l'objet est extrait, vous conservez également la version extraite. Remarque: Après avoir purgé les versions de l'objet, vous ne pouvez pas les récupérer. Pour vous assurer de pouvoir revenir à des versions antérieures, évitez de purger toutes les versions d'un objet.
-t	purge_cutoff_time	Obligatoire si vous n'utilisez pas -d ou -n. Heure limite pour purger les versions des objets actifs. Purge les versions qui ont été archivées avant l'heure limite. Vous pouvez spécifier l'heure limite de purge au format <code>MM/JJ/AAAA HH24:MI:SS</code> , au format <code>MM/JJ/AAAA</code> ou sous la forme d'un nombre de jours avant la date actuelle. Si vous spécifiez un nombre de jours, la valeur doit être un entier supérieur à 0. Lorsque vous utilisez l'option -t, vous conservez la dernière version archivée, même si elle a été archivée après l'heure limite de la purge.
-f	folder_name	Facultatif. Dossier contenant les versions de l'objet qui sont purgées. Si vous ne spécifiez pas un dossier, vous purgez les versions de l'objet de tous les dossiers du référentiel.
-q	query_name	Facultatif. Requête utilisée pour purger les versions de l'objet d'un ensemble spécifique de résultats de requête. Remarque: Si vous utilisez l'option -d, vous purgez toutes les versions des objets supprimés. Pour conserver les versions récentes d'objets supprimés et purger les versions plus anciennes, vous pouvez définir une requête qui renvoie les objets supprimés et utiliser ensuite l'option -q avec -n, -t ou les deux.
-o	outputfile_name	Facultatif. Fichier de sortie permettant d'enregistrer les informations relatives aux versions de l'objet purgé.
-p	-	Facultatif. Affiche un aperçu de la commande <i>PurgeVersion</i> . <i>pmrep</i> affiche les résultats de la purge sans réaliser vraiment la purge des versions de l'objet.
-b	-	Facultatif. Affiche ou enregistre les informations de la purge en mode détaillé. Le mode détaillé fournit des informations détaillées sur les versions de l'objet, notamment le nom de référentiel, le nom de dossier, le numéro de version et l'état. Vous ne pouvez pas utiliser l'option -b avec -o et -p.

Option	Argument	Description
-c	-	Facultatif. Recherche dans les groupes de déploiement du référentiel des références aux versions de l'objet renvoyées dans un aperçu de purge. Si un aperçu de purge contient une version d'objet dans un groupe de déploiement, <i>pmrep</i> affiche un avertissement. Lorsque vous utilisez l'option -c avec l'option -p, la commande répertorie les objets qui sont purgés, puis répertorie les versions d'objet qui sont contenues dans les groupes de déploiement. Lorsque vous utilisez l'option -c sans l'option -p, la commande ne purge pas les versions d'objet qui font partie de groupes de déploiement. Remarque: L'option -c peut avoir un impact négatif sur les performances.
-s	dbd_separator	Facultatif. Si une source ODBC comporte un point (.) dans le nom, définissez un autre caractère de séparation lorsque vous définissez l'objet source. Par exemple, au lieu de database_name.source_name, définissez l'objet source en tant que database_name\source_name et dbd_separator en tant que barre oblique inversée (\).
-k	-	Facultatif. Répertorie tous les noms et toutes les versions d'objet qui n'ont pas été purgés bien qu'ils correspondent aux critères de purge. L'option -k indique également la raison pour laquelle les versions d'objet n'ont pas été purgées. Par exemple, une version d'objet n'est pas purgée si vous ne disposez pas de privilèges suffisants pour purger l'objet. Remarque: Une version d'objet n'est pas purgée lorsqu'elle appartient à un groupe de déploiement. Lorsqu'un objet est un membre de plusieurs groupes de déploiement, la raison répertorie le premier groupe de déploiement qui entraîne l'objet à ne pas être purgé.

Exemples

L'exemple suivant purge toutes les versions de tous les objets supprimés du référentiel :

```
pmrep purgeversion -d all
```

Remarque: Pour des performances optimales, faites une purge au niveau du dossier ou utilisez des critères de purge pour réduire le nombre de versions d'objet purgées. Éviter de purger tous les objets supprimés ou toutes les anciennes versions au niveau du référentiel.

L'exemple suivant purge toutes les versions archivées des objets, sauf la dernière, dans le dossier dossier1 :

```
pmrep purgeversion -n 1 -f folder1
```

L'exemple suivant prévisualise une purge de toutes les versions d'objet qui ont été archivées avant midi, le 5 janvier 2005 et envoie les résultats dans le fichier nommé purge_output.txt :

```
pmrep purgeversion -t '01/05/2005 12:00:00' -o purge_output.txt -p
```

Enregistrement

Enregistre un référentiel local avec un référentiel global connecté. Vous devez vous connecter au référentiel global avant de vous enregistrer dans le référentiel local.

En outre, vous devez exécuter le service de référentiel du référentiel local en mode exclusif. Vous pouvez configurer le service de référentiel pour qu'il s'exécute en mode exclusif dans l'outil Administrator ou vous pouvez utiliser la commande *infacmd* UpdateRepositoryService.

La commande renvoie « inscription correctement terminée » ou renvoie le message « impossible d'exécuter l'inscription ». L'inscription peut échouer pour les raisons suivantes :

- La connexion au service de référentiel a échoué.
- Le référentiel local n'est pas exécuté en mode exclusif.
- Le service de référentiel n'a pas réussi à initialiser les informations au sujet du référentiel global.
- Le service de référentiel n'a pas réussi à inscrire le référentiel local avec le référentiel global.

La commande Register utilise la syntaxe suivante :

```
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)
```

Le tableau suivant décrit les options et arguments de *pmrep* Register :

Option	Argument	Description
-r	local_repository_name	Obligatoire. Nom du référentiel local à enregistrer.
-n	local_repository_user_name	Obligatoire. Nom d'utilisateur local.
-s	local_repository_user_security_domain	Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. La valeur par défaut est Natif.
-x	local_repository_password	Facultatif. Mot de passe de connexion au référentiel local cible. Vous utilisez l'option -x ou -X, mais pas les deux. Si vous n'utilisez pas l'option -x ou -X, <i>pmrep</i> vous demande le mot de passe.
-X	repository_password_environment_variable	Facultatif. Variable d'environnement de mot de passe de connexion pour le référentiel local cible. Vous utilisez l'option -x ou -X, mais pas les deux. Si vous n'utilisez pas l'option -x ou -X, <i>pmrep</i> vous demande le mot de passe.
-d	local_repository_domain_name	Obligatoire si le référentiel local est dans un autre domaine et que vous n'utilisez pas les options -h et -o. Nom du domaine Informatica pour le référentiel.

Option	Argument	Description
-h	local_repository_portal_host_name	Obligatoire si le référentiel local est dans un autre domaine et que vous n'utilisez pas -d. Le nom de la machine du domaine abritant le référentiel local. Si vous utilisez cette option, vous ne pouvez pas utiliser l'option -o.
-o	local_repository_portal_port_numéro	Obligatoire si le référentiel local est dans un autre domaine et que vous n'utilisez pas -d. Le numéro de port pour le domaine abritant le référentiel local. Si vous utilisez cette option, vous devez aussi utiliser l'option -h.

RegisterPlugin

Enregistre un plug-in externe dans un référentiel. L'enregistrement d'un plug-in ajoute ses fonctionnalités au référentiel. Utilisez la commande RegisterPlugin pour mettre à jour les plug-ins existants.

Lorsque vous utilisez cette commande, le service de référentiel doit être exécuté en mode exclusif. Vous pouvez configurer le service de référentiel pour qu'il s'exécute en mode exclusif dans l'outil Administrator ou vous pouvez utiliser la commande *infacmd* UpdateRepositoryService.

La commande RegisterPlugin utilise la syntaxe suivante :

```
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)]
```

Le tableau suivant décrit les options et arguments de *pmrep* RegisterPlugin :

Option	Argument	Description
-i	input_registration_file_name_or_chemin	Requis. Nom ou chemin du fichier d'enregistrement du plug-in.
-e	-	Facultatif. Met à jour un plug-in existant. Non applicable pour les modules d'authentification.
-l	Connexion NIS	Facultatif. Enregistre les composants du module de sécurité. Fournit la connexion NIS de l'utilisateur enregistrant un module de sécurité externe. Si le plug-in contient un module d'authentification, vous devez fournir le nom de la connexion externe, sinon l'inscription échoue. Cette connexion devient le nom de l'administrateur du référentiel. N'utilisez pas cette option pour d'autres plug-ins.

Option	Argument	Description
-w	Mot de passe NIS	Facultatif. Utiliser pour enregistrer les composants du module d'authentification. Mot de passe du répertoire externe de l'utilisateur qui enregistre le module. Si le plug-in contient un module d'authentification, vous devez fournir le mot de passe utilisateur du répertoire externe ou l'inscription échoue. N'utilisez pas cette option pour d'autres plug-ins. Utilisez l'option -w ou -W, mais pas les deux. Si vous ne fournissez pas de mot de passe ou de variable d'environnement de mot de passe, <i>pmrep</i> vous demande un mot de passe.
-W	NIS_password_environment_variable	Facultatif. Utiliser pour enregistrer les composants du module d'authentification. Variable d'environnement de mot de passe du répertoire externe de l'utilisateur enregistrant le module. Si le plug-in contient un module d'authentification, vous devez fournir le mot de passe utilisateur du répertoire externe ou l'inscription échoue. N'utilisez pas cette option pour d'autres plug-ins. Utilisez l'option -w ou -W, mais pas les deux. Si vous ne fournissez pas de mot de passe ou de variable d'environnement de mot de passe, <i>pmrep</i> vous demande un mot de passe.
-k	-	Facultatif. Stocke les CRC de la bibliothèque du plug-in dans le référentiel. Quand le service de référentiel charge le module, il compare la bibliothèque avec le CRC.
-N	-	Enregistre un plug-in. Obligatoire lorsque les conditions suivantes sont vraies : <ul style="list-style-type: none"> - Vous mettez à niveau PowerCenter. - La mise à niveau de PowerCenter n'a pas de nouvelle version de référentiel. - Le plug-in contient les fonctionnalités mises à jour. - Le plug-in est enregistré par défaut avec une nouvelle installation PowerCenter.

Enregistrement d'un module de sécurité

Si vous voulez utiliser un service de répertoire externe pour conserver les utilisateurs et les mots de passe d'un référentiel, vous devez enregistrer le module de sécurité dans le référentiel. Utilisez la commande *Registerplugin* pour enregistrer le plug-in de sécurité.

Exemple

Vous administrez PowerCenter pour une organisation qui a un LDAP NIS centralisé pour l'authentification utilisateur. Lorsque vous mettez à niveau PowerCenter, vous décidez d'utiliser le LDAP pour l'authentification utilisateur. La mise à niveau installe le module de sécurité LDAP dans le dossier de sécurité du référentiel. Après la connexion au référentiel avec la commande *Connect*, l'administrateur exécute la commande *pmrep* pour enregistrer le nouveau module externe dans le référentiel :

```
pmrep registerplugin -i security/ldap_authen.xml -l adminuser -w admpass
```

Les options du nom de connexion -l et du mot de passe de connexion -w contiennent les informations de connexion NIS valides de l'utilisateur exécutant la commande *pmrep*. Après l'enregistrement, vous devez utiliser ce nom de connexion et ce mot de passe pour accéder au référentiel.

Remarque: Le nom de connexion et le mot de passe doivent être valides dans le répertoire externe, sinon l'accès par l'administrateur au référentiel en utilisant LDAP sera impossible.

L'option -i contient le nom du fichier XML qui décrit le module de sécurité.

Restaurer

Vous pouvez restaurer un fichier de sauvegarde de référentiel dans une base de données. La base de données cible doit être vide.

La commande *pmrep Restore* utilise la syntaxe suivante :

```
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)]
```

Le tableau suivant décrit les options et arguments de *pmrep Restore* :

Option	Argument	Description
-u	domain_user_name	Obligatoire. Nom d'utilisateur.
-s	domain_user_security_domain	Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. La valeur par défaut est Natif.
-p	domain_password	Facultatif. Mot de passe. Vous pouvez utiliser l'option -p ou -P, mais pas les deux. Si vous n'utilisez ni l'option -p, ni l'option -P, <i>pmrep</i> vous demande le mot de passe.

Option	Argument	Description
-P	domain_password_ environment_variable	Facultatif. Variable d'environnement de mot de passe. Vous pouvez utiliser l'option -p ou -P, mais pas les deux. Si vous n'utilisez ni l'option -p, ni l'option -P, <i>pmrep</i> vous demande le mot de passe.
-i	input_file_name	Obligatoire. Nom du fichier de sauvegarde du référentiel. Utilisez un nom de fichier et un chemin local pour le service de référentiel.
-g	-	Facultatif. Effectue la promotion du référentiel vers un référentiel global.
-y	-	Facultatif. Active le versionnage d'objet pour le référentiel.
-b	-	Facultatif. Ignore les tables associées au flux de travail et les journaux de session pendant la restauration.
-j	-	Facultatif. Ignore l'historique du groupe de déploiement lors de la restauration.
-q	-	Facultatif. Ignore les tables associées aux données MX lors de la restauration.
-f	-	Facultatif. Ignore les statistiques de tâche lors de la restauration.
-a	-	Facultatif. Crée de nouveaux identifiants de dossier interne pour les dossiers dans le référentiel restauré. Ceci vous permet de copier les dossiers et des groupes de déploiement entre le référentiel d'origine et le référentiel restauré. Si vous n'utilisez pas -a, vous ne pouvez pas copier de dossiers et de groupes de déploiement entre les référentiels originaux et les référentiels restaurés.
-e	-	Facultatif. Quitte si le nom de domaine dans le fichier binaire est différent du nom de domaine actuel

Exemple

L'exemple suivant restaure un référentiel en tant que référentiel avec version et spécifie le nom de l'administrateur et le mot de passe pour conserver l'enregistrement du module de sécurité LDAP.

```
restore -u administrator -p password -i repository1_backup.rep -y
```

RollbackDeployment

Annule un déploiement pour purger les versions déployées d'objets depuis le référentiel cible. Utilisez cette commande pour annuler tous les objets dans un groupe de déploiement que vous avez déployés à une date et une heure spécifiques.

Vous ne pouvez pas annuler une partie d'un déploiement. Pour annuler, vous devez vous connecter au référentiel cible. Vous ne pouvez pas annuler un déploiement depuis un référentiel sans version.

Pour initier un retour en arrière, vous devez annuler la dernière version de chaque objet.

La commande RollbackDeployment utilise la syntaxe suivante :

```
pmrep rollbackdeployment -p <deployment_group_name> -t <nth_latest_deploy_run> -r  
<repository_name> -v <nth_latest_version_of_deployment_group>
```

Le tableau suivant décrit les options et arguments de *pmrep* RollbackDeployment :

Option	Argument	Description
-p	deployment_group_name	Obligatoire. Nom du groupe de déploiement à annuler.
-t	nth_latest_deploy_run	Obligatoire. Version du déploiement que vous souhaitez annuler.
-r	repository_name	Facultatif. Nom du référentiel source à partir duquel vous déployez le groupe de déploiement.
-v	nth_latest_version_of_deployment_group	Facultatif. Version du groupe de déploiement que vous souhaitez annuler.

Exemple

Vous avez un déploiement avec cinq versions et vous souhaitez annuler les deux dernières versions. Pour effectuer cela, vous devez d'abord annuler le dernier déploiement. Entrez le texte suivant à l'invite pour revenir en arrière une fois et purger le dernier déploiement :

```
rollbackdeployment -p Deploy_sales -t 1
```

Ensuite, entrez le texte suivant pour annuler le déploiement suivant le dernier :

```
rollbackdeployment -p Deploy_sales -t 2
```

Exécuter

Ouvre un fichier de script contenant plusieurs commandes *pmrep*, lit chaque commande et les exécute. Si le fichier de script est encodé en UTF-8, vous devez utiliser l'option -u et la page de code du référentiel doit être en UTF-8. Si vous exécutez un fichier de script encodé en UTF-8 qui comprend la commande Connect à un référentiel qui n'a pas une page de code en UTF-8, l'exécution de la commande va échouer.

Si le fichier de script n'est pas encodé en UTF-8, omettez l'option -u. Si vous utilisez l'option -o et l'option -u, *pmrep* génère le fichier de sortie en UTF-8. Si vous utilisez l'option -o et que vous omettez l'option -u, *pmrep* génère le fichier de sortie en fonction des paramètres régionaux du système de la machine où vous exécutez *pmrep*.

La commande renvoie « exécution correctement terminée » ou renvoie le message « Échec de l'exécution ». L'exécution peut échouer si le service de référentiel n'arrive pas à ouvrir le fichier de script ou le fichier de sortie.

La commande Run utilise la syntaxe suivante :

```
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)]`

Le tableau suivant décrit les options et arguments de *pmrep* Run :

Option	Argument	Description
-f	nom du fichier de script	Obligatoire. Nom du fichier de script.
-o	nom du fichier de sortie	Facultatif. Nom du fichier de sortie. Cette option écrit dans le fichier de sortie tous les messages générés par les commandes dans le fichier de script. Si vous utilisez l'option -u et l'option -o, <i>pmrep</i> génère un fichier de sortie encodé en UTF-8. Si vous utilisez l'option -o sans l'option -u, <i>pmrep</i> génère le fichier de sortie en fonction des paramètres régionaux du système de la machine où vous exécutez <i>pmrep</i> .
-e	-	Facultatif. Les commandes sont renvoyées en écho vers le script.
-s	-	Facultatif. Interrompt l'exécution du script après la première erreur.
-u	-	Facultatif. Encode le fichier de sortie au format UTF-8. Si vous utilisez l'option -u et l'option -o, <i>pmrep</i> encode également le fichier de sortie au format UTF-8. Utilisez cette option uniquement si la page de code du référentiel est en UTF-8.

ShowConnectionInfo

Renvoie le nom du référentiel et les informations utilisateur pour la connexion actuelle.

Utilisez la commande ShowConnectionInfo en mode interactif. Lorsque vous vous connectez à un référentiel en mode interactif, *pmrep* conserve les informations de connexion en mémoire jusqu'à ce que vous quittiez le référentiel ou que vous vous connectiez à un autre référentiel.

Lorsque vous utilisez la commande ShowConnectionInfo en mode ligne de commande, un message d'échec d'exécution de la commande est affiché. *pmrep* ne conserve pas les informations de connexion en mode ligne de commande. La commande ShowConnectionInfo ne se connecte pas au référentiel.

La commande ShowConnectionInfo utilise la syntaxe suivante :

```
showconnectioninfo
```

Elle renvoie les informations suivantes :

```
Connected to Repository MyRepository in MyDomain as user MyUserName
```

SwitchConnection

Change le nom d'une connexion existante. Lorsque vous utilisez SwitchConnection, le service de référentiel remplace les connexions de la base de données relationnelle pour toutes les sessions utilisant la connexion de l'un des emplacements suivants :

- Connexion source
- Connexion cible
- Propriété des informations de connexion dans les transformations de recherche
- Propriété des informations de connexion dans les transformations de procédure stockée
- Propriété de session de la valeur de connexion \$Source
- Propriété de session de la valeur de connexion \$Target

Si le référentiel contient à la fois des connexions relationnelles et des connexions d'application avec le même nom et que vous avez indiqué le type de connexion comme relationnel dans *tous* les emplacements du référentiel, le service de référentiel remplace la connexion relationnelle.

Par exemple, vous avez une source relationnelle et une source d'application, toutes les deux appelées ITEMS. Dans une session, vous avez spécifié le nom ITEMS pour une connexion de source relationnelle à la place de Relational:ITEMS. Lorsque vous utilisez SwitchConnection pour remplacer la connexion relationnelle ITEMS par une autre connexion relationnelle, *pmrep* ne remplace aucune connexion relationnelle dans le référentiel, car il ne peut pas déterminer le type de connexion pour la connexion source entrée comme ITEMS.

La commande SwitchConnection utilise la syntaxe suivante :

```
switchconnection  
  
-o <old_connection_name>  
  
-n <new_connection_name>
```

Le tableau suivant décrit les options et arguments de *pmrep* SwitchConnection :

Option	Argument	Description
-o	old_connection_name	Obligatoire. Nom de la connexion que vous voulez modifier.
-n	new_connection_name	Obligatoire. Nouveau nom de connexion.

TruncateLog

Supprime des détails du référentiel. Vous pouvez supprimer tous les journaux, ou supprimer les journaux d'un dossier ou d'un flux de travail. Vous pouvez également saisir une date et supprimer tous les journaux antérieurs à cette date.

La commande renvoie le message « truncateLog terminé avec succès » ou « Impossible d'exécuter truncateLog ». L'opération de troncation peut échouer pour les raisons suivantes :

- Le nom n'est pas valide.
- Le flux de travail n'existe pas dans le dossier spécifié.
- Vous avez indiqué un flux de travail, mais pas de nom de dossier.

La commande TruncateLog utilise la syntaxe suivante :

```
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>]
```

Le tableau suivant décrit les options et les arguments de pmrep TruncateLog :

Option	Argument	Description
-t	logs_truncated	Requis. Utilisez « all » pour supprimer tous les journaux ou entrez une heure de fin. <i>pmrep</i> supprime tous les journaux antérieurs à la date de fin. Vous pouvez spécifier l'heure de fin au format MM/DD/YYYY HH24:MI:SS ou spécifier un nombre de jours avant la date actuelle. Si vous spécifiez le nombre de jours, la date de fin doit être un nombre entier supérieur à 0.
-f	folder_name	Facultatif. Supprime les journaux associés au dossier. Si vous n'indiquez pas le nom du dossier et le nom du flux de travail, <i>pmrep</i> supprime tous les journaux du référentiel.
-w	workflow_name	Facultatif. Supprime les journaux associés au flux de travail. Si vous n'indiquez pas le nom du dossier et le nom du flux de travail, le service de référentiel supprime tous les journaux du référentiel. Si vous indiquez le nom du dossier et le nom du flux de travail, le service de référentiel supprime les journaux associés au flux de travail. Si vous entrez le nom du flux de travail, vous devez aussi fournir le nom du dossier.

UndoCheckout

Inverse l'extraction d'un objet. Lorsque vous annulez une extraction, le référentiel libère le verrou de tentative d'écriture sur l'objet et rétablit la dernière version archivée de l'objet. Si vous souhaitez modifier à nouveau l'objet, vous devez l'extraire.

La commande UndoCheckout utilise la syntaxe suivante :

```
undocheckout  
  
-o <object_type>  
  
[-t <object_subtype>]  
  
-n <object_name>  
  
-f <folder_name>  
  
[-s dbd_separator]
```


Le tableau suivant décrit les options et arguments de *pmrep UndoCheckout* :

Option	Argument	Description
-o	object_type	Obligatoire. Type d'objet. Vous pouvez spécifier la source, la cible, la transformation, le mappage, la session, le worklet, le flux de travail, le planificateur, la configuration de session, la tâche, le cube et la dimension.
-t	object_subtype	Facultatif. Type de transformation ou de tâche. Ignoré pour d'autres types d'objets. Pour plus d'informations sur les sous-types valides, consultez "Liste des types d'objets" à la page 1433 .
-n	object_name	Obligatoire. Nom de l'objet extrait.
-f	folder_name	Obligatoire. Nom du dossier contenant l'objet.
-s	dbd_separator	Facultatif. Si une source ODBC comporte un point (.) dans le nom, définissez un autre caractère de séparation lorsque vous définissez l'objet source. Par exemple, au lieu de database_name.source_name, définissez l'objet source comme database_name\source_name et définissez dbd_separator comme une barre oblique inversée (\).

Désinscrire

Désinscrit un référentiel local depuis un référentiel global connecté.

Pour utiliser cette commande, vous devez exécuter le service de référentiel du référentiel en mode exclusif. Vous pouvez configurer le service de référentiel pour l'exécution en mode exclusif dans l'outil Administrator ou en utilisant la commande *infacmd UpdateRepositoryService*.

La commande renvoie « désinscription terminée avec succès » ou renvoie le message « impossible d'exécuter unregister ». L'inscription peut échouer pour les raisons suivantes :

- Le service de référentiel du référentiel local n'est actuellement pas exécuté en mode exclusif.
- Le service de référentiel n'a pas réussi à initialiser les informations au sujet du référentiel global.
- La connexion au service de référentiel a échoué.

La commande *Unregister* utilise la syntaxe suivante :

```
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)
```

Le tableau suivant décrit les options et arguments de *pmrep* Unregister :

Option	Argument	Description
-r	local_repository_name	Obligatoire. Nom du référentiel local à désinscrire.
-n	local_repository_user_name	Obligatoire. Nom d'utilisateur local.
-s	local_repository_user_security_domain	Obligatoire si vous utilisez une authentification LDAP. Nom du domaine de sécurité auquel appartient l'utilisateur. La valeur par défaut est Natif.
-x	local_repository_password	Requis si vous n'utilisez pas l'option -X. Mot de passe de connexion au référentiel local cible. Vous devez utiliser l'option -x ou -X, mais pas les deux.
-X	local_repository_password_environment_variable	Requis si vous n'utilisez pas l'option -x. Variable d'environnement de mot de passe de connexion pour le référentiel local cible. Vous devez utiliser l'option -x ou -X, mais pas les deux.
-d	local_repository_domain_name	Obligatoire si le référentiel local est dans un autre domaine et que vous n'utilisez pas les options -h et -o. Nom du domaine Informatica pour le référentiel.
-h	local_repository_portal_host_name	Requis si le référentiel local est dans un autre domaine et que vous n'utilisez pas l'option -d. Nom de la machine du domaine où le référentiel local est situé. Si vous utilisez cette option, vous ne pouvez pas utiliser l'option -o.
-o	local_repository_portal_port_numéro	Requis si le référentiel local est dans un autre domaine et que vous n'utilisez pas l'option -d. Numéro de port pour le domaine où le référentiel local est situé. Si vous utilisez cette option, vous devez aussi utiliser l'option -h.

UnregisterPlugin

Supprime un plug-in d'un référentiel. Vous pouvez ajouter et supprimer des plug-ins pour étendre les fonctionnalités du système. Un plug-in est un module logiciel qui introduit de nouvelles métadonnées de référentiel.

Lorsque vous utilisez cette commande, le service de référentiel doit être exécuté en mode exclusif. Vous pouvez configurer le service de référentiel pour qu'il s'exécute en mode exclusif dans l'outil Administrator ou vous pouvez utiliser la commande *infacmd* UpdateRepositoryService.

La commande UnregisterPlugin utilise la syntaxe suivante :

```
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>]]
```

Le tableau suivant décrit les options et arguments de *pmrep* UnregisterPlugin :

Option	Argument	Description
-v	vendor_id	Obligatoire. Identifie le plug-in de sécurité par numéro d'identification du fournisseur. Vous devez définir ce numéro lorsque vous enregistrez le plug-in.
-l	plug-in_id	Obligatoire. Identifie le plug-in par un numéro d'identification. Vous devez définir ce numéro d'identification lorsque vous enregistrez le plug-in.
-s	-	Facultatif. Indique s'il s'agit d'un module de sécurité externe.
-g	-	Facultatif. Applicable lors de l'enregistrement d'un module de sécurité externe. Supprime l'association entre les noms d'utilisateur et les noms de connexion dans le référentiel lorsque vous annulez l'enregistrement d'un module de sécurité externe. Si vous omettez cette option, vous conservez l'association dans le référentiel, mais le gestionnaire du référentiel ne l'affiche nulle part. Utilisez cette option lorsque vous désinscrivez un module de sécurité.
-w	new_password	Requis lorsque le plug-in contient un module de sécurité. Requis si vous n'utilisez pas l'option -W. Vous devez utiliser l'option -w ou -W, mais pas les deux. Indique un nouveau mot de passe pour l'utilisateur exécutant la commande UnregisterPlugin. Lorsque vous annulez l'enregistrement d'un module d'authentification externe, tous les mots de passe des utilisateurs se réinitialisent aux valeurs dans le référentiel. Vous devez entrer un nouveau mot de passe pour accéder au référentiel.
-W	new_password_environment_variable	Requis lorsque le plug-in contient un module de sécurité. Requis si vous n'utilisez pas l'option -w. Vous devez utiliser l'option -w ou -W, mais pas les deux. Indique une nouvelle variable d'environnement mot de passe pour l'utilisateur exécutant la commande d'annulation d'enregistrement. Lorsque vous annulez l'enregistrement d'un module d'authentification externe, tous les mots de passe des utilisateurs se réinitialisent aux valeurs dans le référentiel. Vous devez entrer un nouveau mot de passe pour accéder au référentiel.

Désinscription d'un module de sécurité externe

Utilisez la commande UnregisterPlugin pour arrêter l'utilisation d'un module de sécurité externe avec un référentiel. Si vous désinscrivez le module de sécurité externe, PowerCenter passe en mode d'authentification du référentiel. Tous les mots de passe utilisateur se réinitialisent aux valeurs présentes dans le référentiel à la place des valeurs présentes dans le répertoire externe. Lorsque vous désinscrivez le module de sécurité, vous ne perdez pas le mappage entre les noms d'utilisateur et les noms de connexion de sécurité externe à moins que vous n'entriez l'option -g. Réutilisez le mappage si vous enregistrez un nouveau module de sécurité.

Remarque: Bien que vous puissiez enregistrer les associations entre les connexions externes et les noms d'utilisateur, le gestionnaire de référentiel n'affiche pas les connexions externes quand il s'exécute avec l'authentification utilisateur.

Vous devez utiliser l'option `-w` ou `-W` pour créer un nouveau mot de passe lorsque vous désinscrivez le module de sécurité.

Exemple

En tant qu'administrateur, vous décidez de passer du module de sécurité LDAP à l'authentification du référentiel. Vous supprimez le mappage nom d'utilisateur-connexion. Les utilisateurs que vous avez ajoutés au système dans l'authentification du référentiel peuvent se connecter avec leurs anciens noms d'utilisateur et mots de passe. Les utilisateurs que vous avez ajoutés au référentiel dans la sécurité LDAP ne peuvent pas se connecter jusqu'à ce que vous ayez activé leurs noms d'utilisateur.

Remarque: Vous devez fournir la connexion et le mot de passe LDAP de NIS pour utiliser la commande `UnregisterPlugin`. Vous devez aussi fournir un nouveau mot de passe à utiliser après être repassé à l'authentification de l'utilisateur.

UpdateConnection

Met à jour le nom d'utilisateur, le mot de passe, la chaîne de connexion et les attributs d'une connexion de base de données.

La commande renvoie un message « opération terminée avec succès » ou le message « L'opération a échoué ». Un échec peut se produire pour les raisons suivantes :

- Le type de base de données n'est pas pris en charge.
- L'objet de connexion n'existe pas.
- *pmrep* n'arrive pas à acquérir un verrou sur l'objet.
- L'un des paramètres requis est absent.

La commande `UpdateConnection` utilise la syntaxe suivante :

```
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)]`

Le tableau suivant décrit les options et arguments de *pmrep* UpdateConnection :

Option	Argument	Description
-t	connection_subtype	Requis. Affiche le sous-type de connexion. Par exemple, pour une connexion relationnelle, les sous-types de connexion comprennent Oracle, Sybase et Microsoft SQL Server. Pour les connexions FTP, le sous-type valide est FTP. Pour obtenir une liste de sous-types de connexion prédéfinis, consultez "Sous-types de connexion" à la page 1384 . Remarque: Le sous-type de connexion dans l'option -t doit être valide pour le type de connexion associé spécifié avec l'option -s.
-d	connection_name	Requis. Nom de la connexion à la base de données.
-u	new_user_name	Facultatif. Nom d'utilisateur utilisé pour l'authentification lorsque vous vous connectez à la base de données relationnelle.
-p	new_password	Facultatif. Mot de passe utilisé pour l'authentification lorsque vous vous connectez à la base de données relationnelle. Utilisez l'option -p ou -P, mais pas les deux. Pour spécifier un paramètre dans le mot de passe, ajoutez le préfixe \$Param dans l'option -p et veillez à utiliser l'option -w. N'utilisez pas de signe dollar (\$) ailleurs dans l'option -p et entrez le mot de passe du paramètre sans espace. Par exemple, -p '\$Param_abc' -w
-P	new_password_environment_variable	Facultatif. Variable d'environnement de mot de passe utilisée pour l'authentification lorsque vous vous connectez à la base de données relationnelle. Utilisez l'option -p ou -P, mais pas les deux.
-w	-	Facultatif. Vous permet d'utiliser un paramètre dans l'option de mot de passe. <i>pmrep</i> utilise le mot de passe spécifié avec l'option -p ou -P comme nom du paramètre de session au moment de l'exécution. Valide uniquement si vous utilisez l'option -p ou -P. Si vous n'utilisez pas de paramètre dans l'option de mot de passe, <i>pmrep</i> utilise le mot de passe d'utilisateur spécifié avec l'option -p ou -P.
-x	-	Facultatif. Désactive l'utilisation des paramètres de mot de passe si vous utilisez le paramètre dans le mot de passe. <i>pmrep</i> utilise le mot de passe spécifié avec l'option -p ou -P.
-K	-	Facultatif. Indique que la base de données à laquelle vous vous connectez s'exécute sur un réseau qui utilise l'authentification Kerberos.
-c	new_connection_string	Facultatif. Chaîne de connexion utilisée par le service d'intégration pour se connecter à la base de données relationnelle.
-a	attribute_name	Facultatif. Nom de l'attribut.
-v	new_attribute_value	Requis si vous utilisez l'option -a. Nouvelle valeur d'attribut de la connexion. Entrez « oui » pour activer les nouveaux attributs et « non » pour désactiver les nouveaux attributs.

Option	Argument	Description
-s	connection type application, relational, ftp, loader or queue	Facultatif. Type de connexion. Les types de connexion sont les suivants : <ul style="list-style-type: none"> - Application - FTP - Chargeur - File d'attente - Relationnel La valeur par défaut est Relationnel. Remarque: Le sous-type de connexion dans l'option -t doit être valide pour le type de connexion associé spécifié avec l'option -s.
-l	page de code	Facultatif. Page de code associée à la connexion.
-S	odbc_subtype	Facultatif. Active le sous-type ODBC pour une connexion ODBC. Une connexion ODBC peut être l'un des sous-types ODBC suivants : <ul style="list-style-type: none"> - AWS Redshift - Azure DW - Greenplum - Google BigQuery - PostgreSQL - Snowflake - SAP HANA - Aucun La valeur par défaut est Aucun.

Pour plus d'informations sur les sous-types de connexion, consultez ["Sous-types de connexion" à la page 1384](#).

UpdateEmailAddr

Met à jour les adresses électroniques de notification de session associées aux tâches Email assignées à la session. Si vous n'avez pas préalablement entré une tâche Email en cas de succès ou d'échec, pour la session, la commande ne met pas à jour les adresses électroniques. Vous pouvez mettre à jour les adresses électroniques de notification pour une session non réutilisable avec un nom unique dans le dossier. Vous pouvez entrer des adresses différentes pour recevoir soit des notifications de succès, soit des notifications d'échec. Cette commande requiert que vous vous connectiez à un référentiel.

La commande UpdateEmailAddr utilise la syntaxe suivante :

```
updateemailaddr
-d <folder_name>
-s <session_name>
-u <success_email_address>
-f <failure_email_address>
```

Le tableau suivant décrit les options et arguments de *pmrep* UpdateEmailAddr :

Option	Argument	Description
-d	folder_name	Obligatoire. Nom du dossier de la session.
-s	session_name	Obligatoire. Nom de la session.
-u	success_email_address	Obligatoire. Adresse électronique vers laquelle envoyer les notifications de succès de session.
-f	failure_email_address	Obligatoire. Adresse électronique à laquelle envoyer les notifications d'échec de session.

UpdateSeqGenVals

Met à jour une ou plusieurs des propriétés suivantes pour la transformation Générateur de séquence spécifiée :

- Valeur de départ
- Valeur de fin
- Incrément
- Valeur actuelle

Vous pouvez vouloir mettre à jour des valeurs de séquence lorsque vous déplacez un mappage depuis un environnement de développement vers un environnement de production. Utilisez la commande UpdateSeqGenVals pour mettre à jour des transformations Générateur de séquence réutilisables et non réutilisables. Cependant, vous ne pouvez pas mettre à jour des valeurs pour les instances de transformations Générateur de séquence réutilisables ou des raccourcis vers des transformations Générateur de séquence.

La commande UpdateSeqGenVals utilise la syntaxe suivante :

```
updateseqgenvals
-f <folder_name>
[-m <mapping_name>]
-t <sequence_generator_name>
[-s <start_value>]
[-e <end_value>]
[-i <increment_by>]
[-c <current_value>]
```

Le tableau suivant décrit les options et arguments de *pmrep* UpdateSeqGenVals :

Option	Argument	Description
-f	folder_name	Obligatoire. Nom du dossier.
-m	mapping_name	Nom du mappage. Lorsque vous mettez à jour des valeurs pour une transformation Générateur de séquence non-réutilisable, vous devez inclure le nom du mappage.
-t	sequence_generator_name	Obligatoire. Nom de la transformation Générateur de séquence.
-s	start_value	Facultatif. Valeur de départ de la séquence générée que vous voulez que le service d'intégration utilise si la transformation Générateur de séquence utilise la propriété Cycle. Si vous sélectionnez Cycle dans les propriétés de transformation, le service d'intégration remonte à cette valeur lorsqu'il atteint la valeur finale. Si vous désignez une valeur non valide, <i>pmrep</i> donne un message d'erreur et ne met pas à jour la transformation Générateur de séquence.
-e	end_value	Facultatif. Valeur maximum générée par le service d'intégration. Si le service d'intégration atteint cette valeur lors de la session et que la séquence n'est pas configurée pour faire un cycle, elle fait échouer la session. Si vous désignez une valeur non valide, <i>pmrep</i> affiche un message d'erreur et ne met pas à jour la transformation Générateur de séquence.
-i	increment_by	Facultatif. Différence entre deux valeurs consécutives du port NEXTVAL. Si vous désignez une valeur non valide, <i>pmrep</i> affiche un message d'erreur et ne met pas à jour la transformation Générateur de séquence.
-c	current_value	Facultatif. Valeur actuelle de la séquence. Entrez la valeur que vous voulez que le service d'intégration utilise en tant que première valeur de la séquence. Si vous voulez faire un cycle dans une série de valeurs, la valeur actuelle doit être supérieure ou égale à la valeur de départ et inférieure à la valeur finale. Si vous désignez une valeur non valide, <i>pmrep</i> donne un message d'erreur et ne met pas à jour la transformation Générateur de séquence.

UpdateSrcPrefix

Met à jour le nom du propriétaire pour les tables de la session source. Vous pouvez mettre à jour le nom du propriétaire pour une source ou toutes les sources d'une session. Updatesrcprefix met à jour le nom du propriétaire des tables sources au niveau de la session.

pmrep met à jour les noms du propriétaire de la table source si vous avez précédemment édité le nom de la table source dans les propriétés de session.

La commande UpdateSrcPrefix utilise la syntaxe suivante :

```
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)]
```

Le tableau suivant décrit les options et arguments de *pmrep* UpdateSrcPrefix :

Option	Argument	Description
-f	folder_name	Obligatoire. Nom du dossier contenant la session.
-s	session_name	Obligatoire. Nom de la session contenant les sources à mettre à jour. Pour les sessions réutilisables, entrez le nom de session. Pour les sessions non réutilisables, vous devez également entrer le chemin de la session de la manière suivante : <i>worklet_name.session_name</i> ou <i>workflow_name.session_name</i> .
-t	source_name	Facultatif. Nom de la source à mettre à jour. Si vous omettez cette option, <i>pmrep</i> met à jour tous les noms de propriétaire de la table source dans la session. Lorsque vous incluez l'option -n, vous pouvez entrer le nom de l'instance source comme affiché dans les propriétés de session ou comme délivré par la commande ListTablesBySess. Bien que la commande UpdateSrcPrefix sera exécutée sans l'option -n, incluez l'option -n pour utiliser le nom de l'instance source. Si vous omettez l'option -n, vous devez entrer le nom dbd et le nom de la table source de la façon suivante : <i>dbd_name.source_name</i> . Vous pouvez trouver le nom dbd source dans Designer Navigator. Le concepteur génère le nom dbd à partir du type de source ou du nom de la source de données lorsque vous créez une définition source dans le référentiel.
-p	prefix_name	Obligatoire. Nom du propriétaire dont vous voulez mettre à jour la table source.
-n	-	Facultatif. Correspond à l'argument nom_source avec les noms de l'instance source. Bien que la commande UpdateSrcPrefix sera exécutée sans l'option -n, incluez l'option -n pour utiliser le nom de l'instance source. Lorsque vous n'incluez pas cette option, <i>pmrep</i> compare l'argument nom_source avec les noms de la table source.

UpdateStatistics

Met à jour les statistiques des tables et des index de référentiel.

La commande renvoie le message « commande UpdateStatistics terminée avec succès » ou « échec de la commande UpdateStatistics ».

La commande UpdateStatistics utilise la syntaxe suivante :

```
updatestatistics
```

UpdateTargPrefix

Met à jour le préfixe de nom de table pour les tables de la session cible. Le préfixe de nom de table désigne le propriétaire de la table dans la base de données. Vous pouvez mettre à jour le nom du propriétaire pour une ou toutes les cibles spécifiées dans une session. UpdateTargPrefix met à jour le préfixe du nom de la table cible au niveau de la session.

pmrep met à jour les préfixes du nom de table si vous avez précédemment édité le préfixe du nom de table au niveau de la session.

La commande UpdateTargPrefix utilise la syntaxe suivante :

```
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)]
```

Le tableau suivant décrit les options et arguments de *pmrep* UpdateTargPrefix :

Option	Argument	Description
-f	folder_name	Requis. Nom du dossier contenant la session.
-s	session_name	Requis. Nom de la session contenant les cibles à mettre à jour. Pour les sessions réutilisables, entrez le nom de la session. Pour les sessions non réutilisables, entrez le nom et le chemin de la session, par exemple : <i>worklet_name.session_name</i> ou <i>workflow_name.session_name</i> .
-t	target_name	Facultatif. Nom de la cible à mettre à jour. Si vous omettez cette option, <i>pmrep</i> met à jour tous les préfixes de nom de table dans la session. Lorsque vous incluez l'option -n, vous pouvez entrer le nom de l'instance cible affiché dans les propriétés de la session ou généré par la commande ListTablesBySess. Même si la commande UpdateTargPrefix s'exécute sans l'option -n, incluez cette option pour utiliser le nom de l'instance cible. Lorsque vous omettez l'option -n, vous devez entrer le nom de la table cible à la place du nom de l'instance cible.

Option	Argument	Description
-p	prefix_name	Requis. Préfixe de nom de table que vous souhaitez mettre à jour dans la table cible.
-n	-	Facultatif. Compare l'argument du nom de la cible avec les noms de l'instance cible. Même si la commande UpdateTargPrefix s'exécute sans l'option -n, incluez cette option pour utiliser le nom de l'instance cible. Lorsque vous omettez cette option, <i>pmrep</i> compare l'argument du nom de la cible avec les noms de la table cible.

Mise à niveau

Met à niveau un référentiel vers la dernière version.

La commande Upgrade utilise la syntaxe suivante :

```
upgrade
[-x <repository_password_for_confirmation> |
-X <repository_password_environment_variable_for_confirmation>]
```

Le tableau suivant décrit les options et arguments de *pmrep* Upgrade :

Option	Argument	Description
-x	repository_password_for_confirmation	Facultatif. Mot de passe. Vous pouvez utiliser l'option -x ou -X, mais pas les deux. Si vous n'utilisez ni l'option -x, ni l'option -X, <i>pmrep</i> vous demande une confirmation du mot de passe.
-X	repository_password_environment_variable_for_confirmation	Requis si vous n'utilisez pas l'option -x. Variable d'environnement de mot de passe. Vous devez utiliser l'option -x ou -X, mais pas les deux.

UninstallAbapProgram

Désinstalle le programme ABAP. Désinstallez un programme ABAP lorsque vous ne voulez plus associer le programme à un mappage. La commande désinstalle les programmes depuis le système SAP et supprime les informations du programme correspondantes du référentiel PowerCenter.

La commande UninstallAbapProgram utilise la syntaxe suivante :

```
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)>

```

Le tableau suivant décrit les options et arguments de pmrep UninstallAbapProgram :

Option	Argument	Description
-s	folder_name	Obligatoire. Le nom du dossier qui contient le mappage du programme ABAP que vous voulez désinstaller.
-m	mapping_name	Obligatoire. Nom du mappage.
-v	version_number	Facultatif. Numéro de version du mappage. La valeur par défaut est la dernière version.
-l	log_filename	Facultatif. Nom du fichier journal où la commande écrit les informations ou les messages d'erreur. Par défaut, le fichier journal est stocké dans le répertoire où vous exécutez la commande.
-u	user_name	Obligatoire. Nom d'utilisateur de connexion du système source SAP. Doit être un utilisateur pour lequel vous avez créé une connexion de système source.
-x	mot de passe	Obligatoire. Mot de passe pour le nom d'utilisateur. Utilisez le programme de ligne de commande pmpasswd pour crypter le mot de passe utilisateur.
-c	connect_string	Obligatoire. Entrée DEST définie dans le fichier <code>sapnwrfc.ini</code> pour une connexion à un serveur d'application SAP spécifique ou pour une connexion qui utilise l'équilibrage de charge SAP.
-t	client	Obligatoire. Numéro de client SAP.
-y	langue	Facultatif. Langue de connexion SAP. Doit être compatible avec le code page client PowerCenter. La valeur par défaut est la langue du système SAP.
-p	program_mode (file, stream)	Obligatoire. Mode dans lequel le service d'intégration PowerCenter extrait les données depuis le système SAP. Sélectionnez le fichier ou le flux.

Exemple

L'exemple suivant désinstalle le programme ABAP :

```

uninstallabaprogram -s folder_name -m mapping_name -l logfile_name -u user_name -x
password -c connect_string -t 800 -y EN -p stream

```

Valider

Valide les objets. Vous pouvez délivrer les résultats dans un fichier de sortie persistant ou avec une sortie standard.

Cela affiche également un résumé de validation vers stdout. Le résumé inclut le nombre d'objets valides, d'objets non valides et d'objets ignorés. Le fichier de sortie persistant contient des informations standard, des ID encodés et un contrôle CRC. Vous pouvez enregistrer et archiver les objets qui sont passés de non valides à valides.

Vous pouvez valider les types d'objets suivants :

- Mappages
- Mapplets
- Sessions
- Flux de travail
- Objets worklet

Si vous utilisez un autre type d'objet dans le paramètre d'entrée, *pmrep* renvoie une erreur. Si vous utilisez un mauvais type d'objet dans un fichier d'entrée persistant, *pmrep* renvoie une erreur et ignore l'objet.

Remarque: La commande *pmrep Validate* ne valide pas les raccourcis.

Lorsque vous exécutez *Validate*, vous pouvez délivrer des informations sur l'état de l'objet :

- **valid.** Objets correctement validés.
- **saved.** Objets sauvegardés après validation.
- **skipped.** Raccourcis et objets qui ne requièrent pas de validation.
- **save_failed.** Objets qui n'ont pas été sauvegardés à cause de conflits de verrou ou d'archivage par un autre utilisateur.
- **invalid_before.** Objets non valides avant la vérification de validation.
- **invalid_after.** Objets non valides après la vérification de validation.

Il est impossible d'enregistrer un objet non réutilisable, sauf si vous enregistrez le parent réutilisable de l'objet. Lorsque vous utilisez l'option *-s*, la commande n'enregistre pas les objets non réutilisables validés, sauf si, dans la même commande, vous répertoriez les objets réutilisables qui sont des parents des objets non réutilisables.

La commande *Validate* utilise la syntaxe suivante :

```
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)]
```

Le tableau suivant décrit les options et arguments de *pmrep Validate* :

Option	Argument	Description
-n	object_name	Requis. Nom de l'objet à valider. Cette option ne doit pas être utilisée si vous utilisez l'argument -i. Lors de la validation d'une session non réutilisable, incluez le nom du flux de travail. Entrez le nom du flux de travail ainsi que celui de la session dans le format suivant : <nom du flux de travail>.<nom de l'instance de session> Lorsque vous validez une session non réutilisable dans un worklet non réutilisable, entrez le nom du flux de travail, le nom du worklet et le nom de la session dans le format suivant : <nom du flux de travail>.<nom du worklet>.<nom de l'instance de session>
-o	object_type	Requis si vous n'utilisez pas de fichier d'entrée persistant. Type d'objet à valider. Vous pouvez spécifier un mapplet, un mappage, une session, un worklet et un flux de travail.
-v	version_number	Facultatif. Version de l'objet à valider. La valeur par défaut est la dernière version ou la version extraite de l'objet.
-f	folder_name	Requis. Nom du dossier contenant l'objet.
-i	persistent_input_file	Facultatif. Fichier texte des commandes ExecuteQuery, Validate ou ListObjectDependencies. Contient une liste des enregistrements de l'objet. Vous ne pouvez pas utiliser ce fichier si vous spécifiez des objets à l'aide des arguments -n, -o ou -f.
-s	-	Facultatif. Enregistrez les objets qui sont passés de valides à non valides dans le référentiel.
-k	-	Requis si vous utilisez -s. Archivez les objets enregistrés.
-m	check_in_comments	Requis si vous utilisez l'option -k et que le référentiel actuel requiert des commentaires d'archivage. Ajoutez des commentaires lors de l'archivage d'un objet.
-p	output_option_types	Requis si vous utilisez l'argument -u. Type d'objet à renvoyer au fichier de sortie persistant ou à la commande stdout après validation. Vous pouvez spécifier le statut valid, saved, skipped, save_failed, invalid_before ou invalid_after. Pour entrer une ou plusieurs options, séparez-les par des virgules.
-u	persistent_output_file_name	Requis si vous utilisez l'argument -p. Nom d'un fichier texte de sortie. Si vous entrez un nom de fichier, la requête enregistre les résultats dans un fichier.
-a	append	Facultatif. Ajoute les résultats au fichier de sortie persistant au lieu de le remplacer.

Option	Argument	Description
-c	column_separator	Facultatif. Caractère ou ensemble de caractères utilisé pour séparer les colonnes des métadonnées de l'objet. Utilisez un caractère ou un ensemble de caractères non utilisé dans les noms d'objets du référentiel. Si l'un des noms d'objets du référentiel contient des espaces, évitez d'utiliser des espaces pour séparer les colonnes. Si vous omettez cette option, la commande <i>pmrep</i> utilise une espace unique.
-r	end-of-record_separator	Facultatif. Caractère ou ensemble de caractères utilisé pour spécifier la fin des métadonnées de l'objet. Utilisez un caractère ou un ensemble de caractères non utilisé dans les noms d'objets du référentiel. La valeur par défaut est newline /n.
-l	end-of-listing_indicator	Facultatif. Caractère ou ensemble de caractères utilisé pour spécifier la fin de la liste d'objet. Entrez un caractère ou un ensemble de caractères non utilisé dans les noms d'objets du référentiel. Si vous omettez cette option, la commande <i>pmrep</i> utilise un point.
-b	-	Facultatif. Commentaires. Affiche d'autres informations en plus des informations minimales sur les objets. Si vous omettez cette option, la commande <i>pmrep</i> affiche un format plus court comprenant le type d'objet, le mot réutilisable ou non réutilisable, le nom de l'objet et son chemin. Le format des commentaires inclut le numéro de version et le nom du dossier. Le format court des objets globaux tel que le libellé, la requête, le groupe de déploiement et la connexion inclut le type et le nom de l'objet. Le format des commentaires inclut le nom du créateur et l'heure de création.
-y	-	Facultatif. Affiche le type de base de données des sources et des cibles.

Version

Affiche la version de PowerCenter et les informations sur la marque commerciale et le copyright d'Informatica.

La commande Version utilise la syntaxe suivante :

```
version
```

CHAPITRE 45

Utilisation de l'utilitaire filemanager

Ce chapitre comprend les rubriques suivantes :

- [Présentation de filemanager, 1476](#)
- [copy, 1478](#)
- [copyfromlocal, 1479](#)
- [list, 1480](#)
- [move, 1481](#)
- [remove, 1482](#)
- [rename, 1484](#)
- [watch, 1485](#)

Présentation de filemanager

L'utilitaire filemanager administre les capacités de prétraitement et de surveillance des fichiers pour un écosystème cloud tel qu'Amazon AWS ou Microsoft Azure.

Vous pouvez utiliser l'utilitaire filemanager pour les capacités de prétraitement suivantes :

- Répertoire des fichiers sur un écosystème cloud ;
- Copier des fichiers sur un écosystème cloud ;
- Copier des fichiers d'un système local vers un écosystème cloud ;
- Déplacer des fichiers sur un écosystème cloud ;
- Renommer des fichiers sur un écosystème cloud ;
- Supprimer des fichiers d'un écosystème cloud.

Vous pouvez utiliser l'utilitaire filemanager pour les capacités de surveillance des fichiers suivantes :

- Déclencher un événement de traitement de fichier ;
- Déclencher un flux de travail ou un mappage.

Vous pouvez utiliser l'utilitaire filemanager à partir de l'un des emplacements suivants :

- Répertoire client. Disponible sous `<Infa home>/clients/tools/filemanager`

- Répertoire serveur. Disponible sous `<Infa home>/tools/filemanager`

Options de journalisation

L'utilitaire filemanager fournit les niveaux de gravité de journal suivants à des fins de débogage :

- FINE. Écrit des messages d'incidents graves, d'information et d'avertissement dans le journal. Les messages sans conséquence ou de débogage sont des journaux des demandes utilisateurs.
- SEVERE. Écrit des messages d'incidents graves, d'avertissement et d'erreur dans le journal. Les messages d'incidents graves incluent les pannes système non récupérables, les échecs de connexion et les erreurs de service.
- WARNING. Écrit des messages d'incidents graves, d'avertissement et d'erreur dans le journal. Les messages d'avertissement concernent notamment des pannes système récupérables.
- INFO. Écrit des messages d'incidents graves, d'information, d'avertissement et d'erreur dans le journal. Les messages d'information comprennent des messages de modification des services et du système.

Règles et instructions pour l'utilitaire filemanager

Utilisez les instructions de syntaxe suivantes pour l'utilitaire filemanager :

- Vous devez disposer d'une autorisation de connexion pour exécuter l'utilitaire filewatcher.
- Vous devez définir la variable d'environnement `INFA_TRUSTSTORE` pour le domaine SSL par défaut.
- Les trois premiers paramètres doivent être dans l'ordre : `filemanager <cloud ecosystem> <command>`. Par exemple, `filemanager aws list`
- Utilisez le chemin absolu pour les noms de fichiers.
- Vous ne pouvez pas copier de dossier vide.
- N'utilisez pas `//` dans les commandes `list`, `move` ou `remove`.
- Les commandes `list` ne spécifient pas si l'objet répertorié est un fichier ou un dossier.
- La commande `remove` ne spécifie pas quel fichier a été supprimé. Cela s'applique au stockage ADLS Gen2.
- L'utilitaire filemanager crée un répertoire TAR si le chemin cible n'est pas spécifié dans les commandes `copy`, `move` ou `remove`.
- Utilisez des guillemets doubles lorsque vous spécifiez un modèle pour copier, répertorier, déplacer ou supprimer un fichier. Vous ne pouvez pas utiliser les modèles `{}` `{1|2}` `?`.
- Pour la surveillance des fichiers, le paramètre `-op<other parameters|optional>` doit être à la fin de la syntaxe de la commande.
- Dans l'écosystème cloud Microsoft Azure, la commande `watch` déclenche le mappage avant qu'un fichier ne soit copié. Cela s'applique au stockage ADLS Gen1.
- Utilisez le paramètre `-dn<domainname|optional>` si plusieurs domaines sont configurés dans Informatica Administrator.

copy

Utilisez la commande `copy` pour copier des fichiers sur un écosystème cloud Amazon AWS.

La syntaxe de la commande `filemanager copy` est la suivante :

```
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]
```

Le tableau suivant décrit les options de la commande `filemanager copy` :

Option	Description
-bucketname -bn	Facultatif. Nom du compartiment contenant les fichiers.
-old_filename -fn	Nom du fichier ou du dossier source que vous souhaitez copier.
-new_foldername -nfn	Nom du dossier cible dans lequel vous souhaitez copier les fichiers.
-new_bucketname -nbn	Nom du compartiment dans lequel vous souhaitez copier les fichiers.
-username -un	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine.
-password -pd	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.
security_domainname -sdn	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Le nom de domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est Natif. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Description
-connection -cn	Nom de la connexion dans Informatica Administrator.
-domainname -dn	Facultatif. Nom du domaine Informatica. Requis uniquement si plusieurs domaines sont configurés dans Informatica Administrator.

copyfromlocal

Utilisez la commande `copyfromlocal` pour copier des fichiers d'un système local vers un écosystème cloud.

La syntaxe de la commande `filemanager copyfromlocal` est la suivante :

```
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]
```

Le tableau suivant décrit les options de la commande `filemanager copyfromlocal` :

Option	Description
-bucketname -bn	Facultatif. Nom du compartiment contenant les fichiers ou le dossier. Cette option s'applique à Amazon AWS.
-cloudpath -cp	Chemin d'accès aux fichiers cloud dans lesquels vous souhaitez effectuer la copie. Cette option s'applique à Microsoft Azure.
-localpath -lp	Chemin d'accès aux fichiers ou au dossier source sur un système local que vous souhaitez copier.
-username -un	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine.
-password -pd	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.

Option	Description
security_domainname -sdn	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification native. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-connection -cn	Nom de la connexion dans Informatica Administrator.
-folderpath -fp	Facultatif. Chemin d'accès aux fichiers sur le cloud où vous souhaitez effectuer la copie. Cette option s'applique à Amazon AWS.
-domainname -dn	Facultatif. Nom du domaine Informatica. Requis uniquement si plusieurs domaines sont configurés dans Informatica Administrator.

list

Utilisez la commande `list` pour répertorier les fichiers d'un écosystème cloud.

La syntaxe de la commande `filemanager list` est la suivante :

```
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]
```

Le tableau suivant décrit les options de la commande `filemanager list` :

Option	Description
-bucketname -bn	Facultatif. Nom du compartiment contenant les fichiers. Cette option s'applique à Amazon AWS.
-cloudpath -cp	Chemin d'accès aux fichiers cloud dans lesquels vous souhaitez effectuer la copie. Cette option s'applique à Microsoft Azure.

Option	Description
-pattern -ptn	Modèle générique permettant de faire correspondre et de répertorier les noms de fichiers ou les modèles.
-username -un	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine.
-password -pd	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.
security_domainname -sdn	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Le nom de domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est Natif. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-connection -cn	Nom de la connexion dans Informatica Administrator.
-folderpath -fp	Facultatif. Chemin où répertorier les fichiers sur le cloud. Cette option s'applique à Amazon AWS.
-domainname -dn	Facultatif. Nom du domaine Informatica. Requis uniquement si plusieurs domaines sont configurés dans Informatica Administrator.

move

Utilisez la commande move pour déplacer des fichiers sur un écosystème cloud.

Dans l'écosystème cloud Microsoft Azure, la commande move ne prend pas en charge l'opération de déplacement si le répertoire cible n'est pas présent.

La syntaxe de la commande filemanager move est la suivante :

```
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]
```

Le tableau suivant décrit les options de la commande filemanager move :

Option	Description
-bucketname -bn	Facultatif. Nom du compartiment contenant les fichiers. Cette option s'applique à Amazon AWS.
-old_filename -fn	Chemin du nom du fichier source à partir duquel vous souhaitez déplacer le fichier. Cette option s'applique à Amazon AWS.
-new_folder -nfn	Chemin de l'emplacement de dossier cible vers lequel vous souhaitez déplacer le fichier. Cette option s'applique à Amazon AWS.
-new_bucketname -nbn	Chemin du nom du compartiment cible vers lequel vous souhaitez déplacer le fichier. Cette option s'applique à Amazon AWS.
-source_cloudpath -scp	Chemin de l'emplacement de fichier source dans l'écosystème cloud Microsoft Azure à partir duquel vous souhaitez déplacer le fichier. Cette option s'applique à Microsoft Azure.
-destination_cloudpath -dcp	Chemin de l'emplacement de dossier cible dans l'écosystème cloud Microsoft Azure vers lequel vous souhaitez déplacer le fichier. Cette option s'applique à Microsoft Azure.
-username -un	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine.
-password -pd	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.
security_domainname -sdn	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Le nom de domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est Natif. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
connexion -cn	Nom de la connexion dans Informatica Administrator.
-domainname -dn	Facultatif. Nom du domaine Informatica. Requis uniquement si plusieurs domaines sont configurés dans Informatica Administrator.

remove

Utilisez la commande remove pour supprimer des fichiers d'un écosystème cloud.

La syntaxe de la commande filemanager remove est la suivante :

```
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]

```

Le tableau suivant décrit les options de la commande filemanager remove :

Option	Description
-bucketname -bn	Facultatif. Nom du compartiment contenant les fichiers. Cette option s'applique à Amazon AWS.
-filename -fn	Nom du fichier ou du dossier que vous souhaitez supprimer. Cette option s'applique à Amazon AWS.
-cloudpath -cp	Chemin de l'emplacement de fichier ou de dossier dans l'écosystème cloud Microsoft Azure d'où vous souhaitez supprimer le fichier. Cette option s'applique à Microsoft Azure.
-username -un	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine.
-password -pd	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.
security_domainname -sdn	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel appartient l'utilisateur du domaine. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est Native. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-connection -cn	Nom de la connexion dans Informatica Administrator.
-folderpath -fp	Facultatif. Chemin d'accès aux fichiers sur le cloud d'où vous souhaitez supprimer le fichier. Cette option s'applique à Amazon AWS.
-domainname -dn	Facultatif. Nom du domaine Informatica. Requis uniquement si plusieurs domaines sont configurés dans Informatica Administrator.

rename

Utilisez la commande `rename` pour renommer des fichiers sur un écosystème cloud.

La syntaxe de la commande `filemanager rename` est la suivante :

```
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]
```

Le tableau suivant décrit les options de la commande `filemanager rename` :

Option	Description
-bucketname -bn	Facultatif. Nom du compartiment contenant les fichiers. Cette option s'applique à Amazon AWS.
-old_filename -fn	Chemin d'accès au nom du fichier source ou à l'ancien nom du fichier que vous souhaitez renommer. Cette option s'applique à Amazon AWS.
-new_filename -nfn	Chemin d'accès au fichier cible ou au nouveau nom du fichier.
-cloudpath -cp	Chemin d'accès au fichier cloud où vous souhaitez renommer le fichier. Cette option s'applique à Microsoft Azure.
-username -un	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine.
-password -pd	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.
security_domainname -sdn	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Le nom de domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est Natif. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.

Option	Description
-connection -cn	Nom de la connexion dans Informatica Administrator.
-domainname -dn	Facultatif. Nom du domaine Informatica. Requis uniquement si plusieurs domaines sont configurés dans Informatica Administrator.

watch

Utilisez la commande watch pour surveiller les fichiers qui déclenchent un événement de traitement de fichier, un mappage ou un flux de travail sur un écosystème cloud.

La syntaxe de la commande filemanager watch est la suivante :

```

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

```

Le tableau suivant décrit les options de la commande filemanager watch :

Option	Description
-bucketname -bn	Facultatif. Nom du compartiment contenant les fichiers ou le dossier. Cette option s'applique à Amazon AWS.
-cloudpath -cp	Chemin d'accès aux fichiers cloud que vous souhaitez surveiller. Cette option s'applique à Microsoft Azure.
-pattern -ptn	Modèle générique permettant de faire correspondre et de répertorier les noms de fichiers ou les modèles.
-username -un	Requis si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine.
-password -pd	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse.
security_domainname -sdn	Requis si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Le nom de domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est Natif. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-connection -cn	Nom de la connexion dans Informatica Administrator.
-Domainname -dn	Requis. Nom du domaine qui exécute le service d'intégration de données.
-DIS -sn	Nom du service d'intégration de données qui exécute un mappage ou un flux de travail.
-applicationname -a	Nom de l'application qui contient un flux de travail ou un mappage.
-mappingname -m	Obligatoire si vous souhaitez surveiller un mappage. Nom du mappage à surveiller.
-workflowname -w	Obligatoire si vous souhaitez surveiller un flux de travail. Nom du flux de travail à surveiller.
-watchtime -wt	Facultatif. Durée en minutes de la surveillance du fichier.
-folderpath -fp	Facultatif. Chemin d'accès aux fichiers sur le cloud où vous souhaitez effectuer la copie. Cette option s'applique à Amazon AWS.
-other_parameters -op	Facultatif. Paramètres personnalisés que vous souhaitez utiliser à partir de l'utilitaire infacmd.

CHAPITRE 46

Utilisation de pmrep Files

Ce chapitre comprend les rubriques suivantes :

- [Utilisation de pmrep Files Overview, 1487](#)
- [Utilisation du fichier d'entrée persistant , 1487](#)
- [Utilisation du fichier de contrôle de l'importation d'objet, 1490](#)
- [Exemples du fichier de contrôle de l'importation d'objets, 1494](#)
- [Utilisation du fichier de contrôle de déploiement , 1501](#)
- [Exemples de fichiers de contrôle de déploiement, 1507](#)
- [Conseils d'utilisation de pmrep Files, 1509](#)

Utilisation de pmrep Files Overview

pmrep inclut un ensemble de fichiers de contrôle utilisés pour définir la manière d'importer des objets dans le référentiel. Les paramètres du fichier de contrôle utilisent les mêmes paramètres dans le fichier de contrôle que vous utilisez dans le Client PowerCenter. Vous pouvez utiliser les fichiers de contrôle suivants :

- **Fichier d'entrée persistant.** Utilisez un fichier d'entrée persistant pour spécifier les objets repository que vous voulez traiter.
- **Fichier de contrôle de l'importation d'objet.** Utilisez le fichier de contrôle de l'importation d'objet et spécifiez un ensemble de questions pour aider à définir comment sont importés les objets.
- **Fichier de contrôle de déploiement.** Vous pouvez copier les objets dans un groupe de déploiement dynamique ou statique vers plusieurs dossiers cible du référentiel cible.

Utilisation du fichier d'entrée persistant

Quand vous exécutez *pmrep* avec certaines tâches, utilisez un fichier d'entrée persistant pour spécifier les objets repository que vous voulez traiter. Le fichier d'entrée persistant représente les objets déjà présents dans le référentiel. Vous pouvez créer un fichier d'entrée persistant manuellement ou en utilisant *pmrep*.

Utilisez un fichier d'entrée persistant avec les commandes *pmrep* suivantes :

- **AddToDeploymentGroup.** Ajoutez des objets à un groupe de déploiement.
- **ApplyLabel.** Objets libellés.

- **ExecuteQuery.** Exécutez une requête pour créer un fichier d'entrée persistant. Utilisez le fichier pour les autres commandes *pmrep*.
- **ListObjectDependencies.** Liste des objets de dépendances. Cette commande peut utiliser un fichier d'entrée persistant à traiter et il peut en créer un.
- **MassUpdate.** Met à jour les propriétés de session pour un ensemble de sessions.
- **ObjectExport.** Exportez des objets dans un fichier XML.
- **Valider.** Validez des objets. Cette commande peut utiliser un fichier d'entrée persistant à traiter et il peut en créer un.

Le fichier d'entrée persistant utilise le format suivant :

```
encoded ID, foldername, object_name, object_type, object_subtype, version_number,
reusable|non-reusable
```

Création d'un fichier d'entrée persistant avec pmrep

Vous pouvez créer un fichier d'entrée persistant à l'aide des commandes *ExecuteQuery*, *Validate* ou *ListObjectDependencies* *pmrep*. Ces commandes créent des fichiers qui contiennent une liste d'objets avec des identifiants encodés et une valeur de contrôle de redondance cyclique (CRC). Elle contient également un GUID du référentiel crypté. Cet identifiant identifie le référentiel d'où provient l'enregistrement.

Les commandes *pmrep* qui utilisent un fichier d'entrée persistant obtiennent les informations de l'objet à partir des identifiants encodés. Les identifiants codés permettent à *pmrep* de traiter le fichier d'entrée rapidement.

Lorsque vous créez un fichier d'entrée persistant avec *pmrep*, il crée le fichier dans le répertoire d'installation de *pmrep*. Vous pouvez spécifier un chemin différent.

Le texte suivant montre un exemple de fichier d'entrée persistant :

```
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
```

Exemple

Vous pouvez utiliser la commande *ExecuteQuery* pour créer un fichier d'entrée persistant d'objets à traiter dans une autre commande *pmrep*. Par exemple, vous souhaitez exporter tous les objets logiquement supprimés dans le référentiel. Vous pourriez créer une requête appelée *find_deleted_objects*. Lorsque vous exécutez la requête avec la commande *pmrep*, comme illustré ici, celle-ci recherche tous les objets supprimés dans le référentiel et exporte les résultats dans un fichier d'entrée persistant :

```
ExecuteQuery -q find_deleted_objects -t private -u deletes_workfile
```

Vous pouvez ensuite utiliser *deletes_workfile* comme fichier d'entrée persistant pour *ObjectExport* :

```
ObjectExport -i deletes_workfile -u exported_del_file
```

ObjectExport exporte tous les objets référencés dans un fichier XML appelé *exported_del_file*.

Création manuelle d'un fichier d'entrée persistant

Si vous souhaitez exécuter des commandes *pmrep* sur un ensemble d'objets que vous ne pouvez pas identifier à l'aide de commandes comme *ExecuteQuery*, vous pouvez créer manuellement un fichier d'entrée.

Utilisez les règles et directives suivantes lorsque vous créez un fichier d'entrée persistant :

- Entrez « none » pour l'ID encodé. Les commandes *pmrep* obtiennent des informations d'objet à partir d'autres arguments dans les enregistrements.
- Pour les objets source, entrez le nom de l'objet comme <DBD_name>.<source_name>.
- Pour les objets, tels que les mappages, qui n'ont pas de sub_type, entrez « none » pour object_subtype ou laissez-le vide. Pour plus d'informations sur les types de transformations et de tâches valides, consultez ["Liste des types d'objets" à la page 1433](#).
- Pour les référentiels avec version, entrez le numéro de version de l'objet que vous voulez ou entrez « LATEST » pour utiliser la dernière version de l'objet.
- Pour les référentiels sans versions, laissez l'argument version_number vide.
- Pour les types d'objets, tels que les cibles, qui ne sont pas réutilisables ou non réutilisables, abandonnez l'argument.
- Vous ne pouvez pas inclure d'objets non réutilisables. Vous pouvez spécifier le parent réutilisable de l'objet non réutilisable.

Par exemple, vous voulez lister les dépendances d'objet non réutilisable pour une transformation filtre. Vous pouvez spécifier le mappage qui est l'objet parent de la transformation:

```
none,CAPO,m_seqgen_map,mapping,none,1,reusable
```

Le mappage *m_seqgen_map* est le parent réutilisable de la transformation filtre. La commande fonctionne correctement lorsque vous spécifiez le parent réutilisable.

Remarque: Lorsque vous utilisez un fichier d'entrée persistant créé manuellement, le service de référentiel renvoie un message indiquant que l'id n'est pas valide. Ceci est un message d'information. Le service de référentiel reconnaît que ceci est un fichier d'entrée créé manuellement et qu'il peut traiter la commande avec « Aucune » comme ID.

Exemple

L'exemple suivant montre un fichier d'entrée persistant créé manuellement :

```
none,EXPORT,CustTgt,target,none,2
none,EXPORT,S_Orders,session,,2,reusable
none,EXPORT,EXP_CalcTot,transformation,expression,LATEST,reusable
```

Dans le premier enregistrement, *CustTgt* est une définition cible. Les cibles n'ont pas de sous-type, de sorte que vous entrez « Aucun » pour l'argument *object_subtype*. Une cible ne peut pas être réutilisable ou non réutilisable, de sorte que vous supprimez l'argument réutilisable. Notez que l'enregistrement dispose de six arguments au lieu de sept.

Dans le deuxième enregistrement, *S_Orders* est une session. Les sessions n'ont pas de sous-type, de sorte que vous laissez l'argument vide.

Dans le troisième enregistrement, vous avez besoin de la dernière version de la transformation, de sorte que vous entrez « LATEST » pour l'argument *version_number*.

Utilisation du fichier de contrôle de l'importation d'objet

Quand vous utilisez la commande *pmrep* ObjectImport, vous pouvez fournir un fichier de contrôle pour répondre aux questions que vous adressez normalement quand vous importez des objets via l'assistant d'importation. Pour créer un fichier de contrôle, vous devez créer un fichier XML défini par *impcntl.dtd*. Le fichier de contrôle de l'importation est installé avec le Client PowerCenter et vous devez inclure son emplacement dans le fichier d'entrée XML.

Voici un exemple de fichier *impcntl.dtd* :

```
<!-- 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 (LAELOBJECT | QUERYOBJECT | TYPEOBJECT | SPECIFICOBJECT)*>

<!--LAELOBJECT allows objects in the target with label name to apply replace/reuse upon
conflict -->
<!ELEMENT LAELOBJECT EMPTY>
<!ATTLIST LAELOBJECT
    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-->
    <!--EXTRANE 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>

```

Paramètres du fichier de contrôle de l'importation d'objets

Le tableau suivant présente les paramètres du fichier de contrôle de l'importation d'objets *pmrep* :

Élément	Nom d'attribut	Description de l'attribut
IMPORTPARAMS	CHECKIN_AFTER_IMPORT	Obligatoire si le versionnage est activé. Archive les objets si leur importation réussit.
IMPORTPARAMS	CHECKIN_COMMENTS	Facultatif. Applique les commentaires aux objets archivés.
IMPORTPARAMS	APPLY_LABEL_NAME	Facultatif. Applique le libellé sur les objets importés.
IMPORTPARAMS	RETAIN_GENERATED_VALUE	Obligatoire si vous utilisez des transformations Générateur de séquence, Normaliseur ou Qualificateur de source XML. Conserve les valeurs actuelles des transformations Générateur de séquence, Normaliseur et Qualificateur de source XML existantes dans la destination.
IMPORTPARAMS	COPY_SAP_PROGRAM	Facultatif. Copie des informations du programme SAP dans le référentiel cible.

Élément	Nom d'attribut	Description de l'attribut
IMPORTPARAMS	APPLY_DEFAULT_CONNECTION	Facultatif. Applique la connexion par défaut lorsqu'une connexion utilisée par une session n'existe pas dans le référentiel cible. La connexion par défaut est la première connexion dans la liste triée des connexions disponibles. Trouve la liste des connexions dans le Gestionnaire de flux de travail.
FOLDERMAP	SOURCEFOLDERNAME	Obligatoire. Importation du nom de dossier pour le faire correspondre à un dossier dans le référentiel cible.
FOLDERMAP	SOURCEREPOSITORYNAME	Obligatoire. Référentiel contenant le dossier source.
FOLDERMAP	TARGETFOLDERNAME	Obligatoire. Nom du dossier cible à utiliser pour la correspondance.
FOLDERMAP	TARGETREPOSITORYNAME	Obligatoire. Référentiel contenant le dossier cible.
TYPEFILTER	TYPENAME	Facultatif. Importe les objets depuis un nœud spécifique, tel que des sources, des cibles ou des mappages.
RESOLVECONFLICT	Éléments LABELOBJECT, QUERYOBJECT, TYPEOBJECT et SPECIFICOBJECT.	Vous pouvez spécifier des résolutions de conflits pour les objets.
LABELOBJECT	LABELNAME	Obligatoire. Identifie les objets par leur libellé pour la spécification de la résolution de conflit.
LABELOBJECT	RESOLUTION	Obligatoire. Remplacer, Réutiliser, Renommer.
QUERYOBJECT	QUERYNAME	Obligatoire. Identifie les objets de cette requête pour la spécification de résolution de conflit.
QUERYOBJECT	RESOLUTION	Obligatoire. Remplacer, Réutiliser ou Renommer.
TYPEOBJECT	OBJECTTYPENAME	Obligatoire. Type d'objet pour cette résolution de conflit. Pour une liste des types d'objets, consultez "Paramètres du fichier de contrôle de l'importation d'objets" à la page 1491 .
TYPEOBJECT	RESOLUTION	Obligatoire. Remplacer, Réutiliser ou Renommer.

Élément	Nom d'attribut	Description de l'attribut
SPECIFICOBJECT	NAME	Obligatoire. Nom d'objet spécifique pour cette résolution de conflit.
SPECIFICOBJECT	DBDNAME	Facultatif. Source DBD pour identifier l'objet source.
SPECIFICOBJECT	OBJECTTYPENAME	Obligatoire. Type d'objet pour cette résolution de conflit. Pour une liste des types d'objets, consultez "Paramètres du fichier de contrôle de l'importation d'objets" à la page 1491.
SPECIFICOBJECT	FOLDERNAME	Obligatoire. Dossier source qui contient l'objet.
SPECIFICOBJECT	REPOSITORYNAME	Obligatoire. Service d'archives source contenant l'objet.
SPECIFICOBJECT	RESOLUTION	Obligatoire. Remplacer, Réutiliser ou Renommer.

Vous pouvez utiliser les types d'objet suivants avec l'attribut OBJECTTYPENAME :

- Tout
- Agrégation
- Qualificateur de source d'applications multigroupe
- Qualificateur de source d'application
- Assignment
- Commande
- Contrôle
- Transformation personnalisée
- Décision
- Courriel
- Event raise
- Event wait
- Expression
- Procédure externe
- Filtre
- Transformation d'entrée
- Jointure
- Procédure de recherche
- Mappage
- Mapplet
- Qualificateur de source MQ
- Normaliseur

- Transformation de sortie
- Rang
- Routeur
- Planificateur
- Session
- Séquence
- SessionConfig
- Trieur
- Définition de source
- Qualificateur de source
- Début
- Définition de cible
- Minuteur
- Contrôle de la transaction
- Stratégie de mise à jour
- Fonction définie par l'utilisateur
- Flux de travail
- Worklet
- Qualificateur de source XML

Remarque: Utilisez le type d'objet « Tout » pour réutiliser ou remplacer tous les objets.

Exemples du fichier de contrôle de l'importation d'objets

Les paramètres que vous spécifiez dans le code du fichier de contrôle déterminent les actions qui se produisent lorsque vous exécutez la commande `ObjectImport` dans *pmrep*. Les exemples suivants discutent d'instances dans lesquelles vous utilisez la commande `ObjectImport` avec un fichier de contrôle pour importer des objets du référentiel. Les éléments et les noms d'attribut qui sont essentiels à la réalisation des tâches décrites sont désignés par des commentaires dans le code.

Le tableau suivant fournit une description des exemples de fichiers de contrôle de l'importation d'objets :

Fonction	Description
Importation d'objets source.	Utilisez l'élément <code>TYPEFILTER</code> pour importer uniquement les objets source.
Importation de plusieurs objets dans un dossier.	Utilisez les éléments <code>IMPORTPARAMS</code> et <code>FOLDERMAP</code> pour importer plusieurs objets.
Archivage et libellé d'objets importés.	Utilisez les attributs <code>CHECKIN_AFTER_IMPORT</code> et <code>APPLY_LABEL_NAME</code> de l'élément <code>IMPORTPARAMS</code> pour libeller des objets importés.

Fonction	Description
Conserver les valeurs des transformations Générateur de séquence et Normaliseur.	Utilisez l'attribut RETAIN_GENERATED_VALUE de l'élément IMPORTPARAMS pour conserver les valeurs Générateur de séquence et Normaliseur lorsque vous importez des objets.
Importation d'objets et d'objets raccourci locaux dans le même référentiel.	Utilisez tous les attributs de l'élément FOLDERMAP pour importer des objets et des objets raccourci locaux qui référencent les objets.
Importation d'objets raccourci depuis un autre référentiel.	Utilisez tous les attributs de l'élément FOLDERMAP pour importer des objets raccourci depuis un autre référentiel.
Importation d'objets dans plusieurs dossiers.	Utilisez tous les attributs de l'élément FOLDERMAP pour importer des objets dans plusieurs dossiers.
Importation d'objets spécifiques.	Utilisez l'élément TYPEFILTER pour importer des objets source spécifiques.
Réutilisation et remplacement d'objets dépendants.	Utilisez les attributs OBJECTTYPENAME et RESOLUTION de l'élément TYPEOBJECT pour réutiliser et remplacer des objets dépendants.
Remplacement de mappages non valides.	Utilisez l'élément QUERYOBJECT pour remplacer les mappages non valides.
Changer le nom des objets.	Utilisez l'attribut RESOLUTION de l'élément SPECIFICOBJECT pour renommer les objets.
Copie de mappages SAP et d'informations du programme SAP.	Utilisez l'attribut COPY_SAP_PROGRAM de l'élément IMPORTPARAMS pour copier des mappages SAP et des informations du programme SAP.
Application d'attributs de connexion par défaut.	Utilisez l'attribut APPLY_DEFAULT_CONNECTION de l'élément IMPORTPARAMS pour appliquer les attributs de connexion par défaut.
Résolution des conflits d'objets.	Utilisez l'élément RESOLVECONFLICT pour résoudre les conflits d'objets.

Importation d'objets source

Vous pouvez importer des objets source. Par exemple, vous souhaitez remplacer tous les objets dupliqués nommés « Monthend » dans le dossier cible. Cependant, vous souhaitez renommer des objets source en conflit qui contiennent « Yr_End » dans le nom d'objet. Vous avez une requête nommée « yr_end_qry » qui trouve ces objets.

Vous pourriez créer un fichier de contrôle avec les attributs suivants :

```
<?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>
```

Importation de plusieurs objets dans un dossier

Vous pouvez importer plusieurs objets dans un dossier, les archiver et les libeller. Par exemple, vous souhaitez importer les objets dans le dossier SRC_F1 et appliquer le libellé LABEL_IMPORT_NEW aux objets.

Vous pourriez créer un fichier de contrôle avec les attributs suivants :

```
<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>
```

Archivage et libellé d'objets importés

Vous pouvez importer des objets dans un dossier, les archiver, les libeller et résoudre le conflit entre les objets de configuration de la session. Par exemple, vous souhaitez exporter les objets du dossier SRC_F1 et les importer dans le dossier TGT_F1. Le service de référentiel crée une configuration de session dans le dossier cible par défaut. Vous incluez l'attribut APPLY_LABEL_NAME dans l'élément IMPORTPARAMS pour libeller les objets importés et l'élément RESOLVECONFLICT dans le fichier de contrôle pour résoudre le conflit.

Vous pourriez créer un fichier de contrôle avec les attributs suivants :

```
<?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>
```

Conserver les valeurs Générateur de séquence et Normaliseur

Vous pouvez conserver les valeurs des transformations Générateur de séquence et Normaliseur lorsque vous importez des objets en remplaçant tous les objets déjà présents dans le dossier cible.

Vous pourriez créer un fichier de contrôle avec les attributs suivants :

```
<?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 OBJECTTYPE="ALL" RESOLUTION="REPLACE"/>
</RESOLVECONFLICT>
</IMPORTPARAMS>
```

Importation d'objets et d'objets raccourci locaux dans le même référentiel

Vous pouvez importer des objets et leurs objets raccourci locaux respectifs dans le même référentiel. Par exemple, vous avez des dossiers nommés SRC_SHARED_F1 et SRC_NONSHARED_F1. Le dossier SRC_NONSHARED_F1 n'est pas partagé et contient des objets raccourci locaux qui font référence à des objets dans le dossier SRC_SHARED_F1. Vous voulez importer les objets dans différents dossiers dans le référentiel cible et vous souhaitez rediriger les objets du dossier raccourci TGT_NONSHARED_F1 vers les objets dans TGT_SHARED_F1.

Vous pourriez créer un fichier de contrôle avec les attributs suivants :

```
<?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>
```

Importation d'objets raccourci depuis un autre référentiel

Vous pouvez importer des objets à partir d'autres référentiels. Par exemple, vous avez des dossiers dans un référentiel local qui contiennent des raccourcis vers des objets dans un référentiel global. Vous souhaitez importer les objets raccourci global vers un référentiel qui est enregistré dans le référentiel global et maintenir des raccourcis vers les objets d'origine dans le référentiel global.

Vous pourriez créer un fichier de contrôle avec les attributs suivants :

```
<?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>
```

Importation d'objets dans plusieurs dossiers

Vous pouvez importer des objets dans plusieurs dossiers qui ont été exportés depuis plusieurs dossiers. Par exemple, vous avez exporté des objets depuis les dossiers SRC_F1, SRC_F2 et SRC_F3 que vous souhaitez importer dans les dossiers cibles TGT_F1, TGT_F2, TGT_F3 dans le référentiel TGT_REPO1.

Vous pourriez créer un fichier de contrôle avec les attributs suivants :

```
<?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>

```

Importation d'objets spécifiques

Vous pouvez choisir les objets que vous souhaitez importer. Par exemple, vous avez exporté plusieurs types d'objets dans un fichier XML. Vous souhaitez importer uniquement des mappages et leurs sources et cibles respectives, dans un dossier.

Vous pourriez créer un fichier de contrôle avec les attributs suivants :

```

<?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_EX_1"/>

<!-- use the TYPENAME attribute to import only mappings -->
  <TYPEFILTER TYPENAME="MAPPING"/>
</IMPORTPARAMS>

```

Réutilisation et remplacement d'objets dépendants

Vous pouvez importer des sessions, remplacer des mappages et réutiliser les sources et cibles existantes dans le dossier cible. Par exemple, vous souhaitez remplacer les mappages et réutiliser les définitions sources, les définitions cibles et les objets de configuration de la session.

Vous pourriez créer un fichier de contrôle avec les attributs suivants :

```

<?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 OBJECTTYPE = "SESSIONCONFIG" RESOLUTION="REUSE"/>

<!-- replace some object types and reuse remaining objects-->
<TYPEOBJECT OBJECTTYPE = "ALL" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPE = "SOURCE DEFINITION" RESOLUTION="REPLACE"/>
<TYPEOBJECT OBJECTTYPE = "MAPPING" RESOLUTION="REPLACE"/>

</RESOLVECONFLICT>
</IMPORTPARAMS>

```

Remarque: Lorsque vous réutilisez ou remplacez un type d'objet, la résolution pour ce type d'objet remplace la résolution de tous les types d'objets. L'exemple précédent remplace les définitions et les mappages source et réutilise les objets restants. Utilisez le type d'objet « Tout » pour réutiliser ou remplacer tous les objets. Pour plus d'informations sur les types d'objets, consultez ["Paramètres du fichier de contrôle de l'importation d'objets" à la page 1491](#).

Remplacement de mappages non valides

Vous pouvez remplacer les mappages non valides et les objets enfants associés qui sont renvoyés par une requête. Par exemple, vous souhaitez remplacer les objets renvoyés par la requête QUERY_PARENT_RENAME.

Vous pourriez créer un fichier de contrôle avec les attributs suivants :

```
<?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" SOURCEREPOSITORYNAME="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>
```

Changement de nom d'objets

Vous pouvez renommer des objets spécifiques lorsque des conflits d'objets surviennent. Par exemple, vous souhaitez renommer les objets ADDRESS, ADDRESS1, R_LKP, MAP_MLET, R_S3 et WF_RS1. Le service de référentiel ajoute un numéro aux noms d'objets.

Vous pourriez créer un fichier de contrôle avec les attributs suivants :

```
<?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" SOURCEREPOSITORYNAME="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" OBJECTTYPE="Source Definition"
  FOLDERNAME="PMREP_CHECKED_OUT" REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
  <SPECIFICOBJECT NAME="ADDRESS1" OBJECTTYPE="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>
```

Copie de mappages SAP et d'informations du programme SAP

Vous pouvez copier des informations du programme SAP lorsque vous importez des mappages SAP. Par exemple, vous souhaitez importer des mappages SAP et copier les informations du programme associées à l'objet que vous importez dans le dossier TGT_F1.

Vous pourriez créer un fichier de contrôle avec les attributs suivants :

```
<?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" SOURCEPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="REPO_EX_1"/>
</IMPORTPARAMS>
```

Application d'attributs de connexion par défaut

Vous pouvez appliquer des attributs de connexion par défaut à une session si une connexion n'est pas présente dans le référentiel cible. Par exemple, aucune connexion n'existe dans le référentiel cible REPO_EX_1.

Vous pourriez créer un fichier de contrôle avec les attributs suivants :

```
<?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" SOURCEPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="REPO_EX_1"/>
<RESOLVECONFLICT>
<SPECIFICOBJECT NAME="R_S3" OBJECTTYPE="Session" FOLDERNAME="PMREP_CHECKED_OUT"
REPOSITORYNAME="REPO_EX_1" RESOLUTION="REPLACE"/>
</RESOLVECONFLICT>
</IMPORTPARAMS>
```

Résolution des conflits d'objets

Vous pouvez résoudre les conflits d'objets pour les objets libellés dans le référentiel cible. Par exemple, vous avez des mappages, mapplets, sources et cibles libellés LBL_MPNG_MPLTS_SRCS_TGTS. Vous souhaitez remplacer ces objets et les libeller REPLACE_LBL_MPNG_MPLTS_SRCS_TGTS et réutiliser toutes les transformations.

Vous pourriez créer un fichier de contrôle avec les attributs suivants :

```
<?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" SOURCEPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="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>

```

Utilisation du fichier de contrôle de déploiement

Un fichier de contrôle de déploiement est un fichier XML que vous utilisez avec les commandes *pmrep* *DeployFolder* et *DeployDeploymentGroup* pour déployer un dossier ou un groupe de déploiement. Vous pouvez créer un fichier de contrôle de déploiement manuellement pour fournir les paramètres pour le déploiement, ou vous pouvez créer un fichier de contrôle de déploiement avec l'assistant Copy.

Si vous créez le fichier de contrôle de déploiement manuellement, il doit être conforme au fichier *depcntl.dtd* qui est installé avec le Client PowerCenter. Vous devez inclure l'emplacement du fichier *depcntl.dtd* dans le fichier de contrôle de déploiement.

Vous pouvez spécifier un délai de dépassement de déploiement dans le fichier de contrôle de déploiement. Le délai de dépassement de déploiement est le temps (en secondes) passé par *pmrep* à attendre l'acquisition des verrous d'objet dans le référentiel cible. Par défaut, *pmrep* attend indéfiniment jusqu'au moment où il acquiert les verrous ou que vous annulez le déploiement. Pour annuler un déploiement pendant l'attente de l'acquisition des verrous par *pmrep*, appuyez sur Ctrl+C.

Remarque: Vous devez créer le fichier de contrôle de déploiement manuellement pour utiliser des paramètres de déploiement tels que *DEPLOYTIMEOUT*.

Voici un exemple de fichier *depcntl.dtd* :

```

<!ELEMENT DEPLOYPARAMS (DEPLOYFOLDER?, DEPLOYGROUP?)>
<!--ATTLIST DEPLOYPARAMS
      DEFAULTSERVERNAME      CDATA      #IMPLIED
      COPYPROGRAMINFO        (YES | NO) "YES"
      COPYMAPVARPERVALS      (YES | NO) "NO"
      RETAINMAPVARPERVALS    (YES | NO) "NO"
      COPYWFLOWVARPERVALS    (YES | NO) "NO"
      COPYWFLOWSESSLOGS      (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"
      OVERRIDESERVER          (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

```

Paramètres du fichier de contrôle de déploiement

Le tableau suivant présente les paramètres du fichier de contrôle de déploiement *pmrep* :

Élément	Nom de l'attribut	Description de l'attribut
DEPLOYPARAMS	DEFAULTSERVERNAME	Requis si vous utilisez DeployFolder et DeployDeploymentGroup et que vous définissez OVERRIDESEVER sur Oui. Le service d'intégration est enregistré dans le référentiel cible pour exécuter les flux de travail déployés. Pour tout déploiement, vous pouvez spécifier un seul service d'intégration.
-	COPYPROGRAMINFO	Facultatif. Copie le programme ABAP installé par SAP.
-	COPYMAPVARPERVALS	Facultatif. Copie les valeurs persistantes de la variable de mappage en fonction des valeurs définies pour RETAINMAPVARPERVALS. Si vous ne définissez pas COPYMAPVARPERVALS ou si vous définissez sa valeur sur Non, les valeurs RETAINMAPVARPERVALS sont ignorées. Pour plus d'informations, consultez la rubrique "Variables de mappage persistantes" à la page 1507 .
-	RETAINMAPVARPERVALS	Facultatif. Conserve les valeurs persistantes de la variable de mappage dans la cible en fonction des valeurs définies pour COPYMAPVARPERVALS. Si vous ne définissez pas COPYMAPVARPERVALS ou si vous définissez sa valeur sur Non, les valeurs RETAINMAPVARPERVALS sont ignorées. Pour plus d'informations, consultez la rubrique "Variables de mappage persistantes" à la page 1507 .
-	COPYWFLOWVARPERVALS	Facultatif. Copie les valeurs persistantes de la variable de flux de travail.
-	COPYWFLOWSESSLOGS	Facultatif. Copie les journaux de flux de travail.
-	COPYDEPENDENCY	Facultatif. Copie les informations de dépendance des objets présents dans les mappages.
-	COPYDEPLOYMENTGROUP	Facultatif. Copie le groupe de déploiement ainsi que les objets correspondants dans le référentiel cible.
-	VALIDATETARGETREPOSITORY	Facultatif. Valide les objets du référentiel cible.
-	LATESTVERSIONONLY	Facultatif. Copie la dernière version.

Élément	Nom de l'attribut	Description de l'attribut
-	CHECKIN_COMMENTS	Facultatif. Annule le commentaire par défaut et en ajoute un autre dans le référentiel cible lors de la copie ou du déploiement d'un objet. Vous devez définir LATESTVERSIONONLY sur True pour pouvoir utiliser cet attribut.
-	DEPLOYTIMEOUT	Facultatif. Durée (en secondes) des tentatives de la commande <i>pmrep</i> pour acquérir les verrous sur les objets du référentiel cible. Une valeur de 0 entraîne l'échec immédiat de l'opération de copie si la commande <i>pmrep</i> ne peut pas obtenir de verrou. Une valeur de -1 indique à la commande <i>pmrep</i> d'attendre indéfiniment jusqu'à ce qu'il acquière les verrous ou que l'utilisateur annule l'opération. La valeur par défaut est -1.
-	RETAINGENERATEDVAL	Facultatif. Conserve la valeur actuelle des transformations Générateur de séquence ou Normalisateur.
-	RETAINSERVERNETVALS	Facultatif. Conserve les valeurs liées au réseau du serveur dans les tâches.
	OVERRIDESEVER	<p>Facultatif. Utilisez cette valeur avec DEFAULTSERVERNAME. Si vous attribuez à OVERRIDESEVER la valeur Oui, l'opération de déploiement attribue le nom de service d'intégration que l'attribut DEFAULTSERVERNAME spécifie pour exécuter les flux de travail déployés. Si l'attribut DEFAULTSERVERNAME n'est pas spécifié ou qu'il contient un nom de service d'intégration non valide, l'opération de déploiement n'attribue pas un service d'intégration aux flux de travail déployés.</p> <p>Si vous attribuez à OVERRIDESEVER la valeur Non, l'opération de déploiement vérifie si elle peut attribuer un service d'intégration aux flux de travail en fonction du service d'intégration dans les référentiels source et cible. Si le même nom de service d'intégration s'affiche dans les référentiels source et cible, l'opération de déploiement attribue le nom de service d'intégration aux flux de travail déployés. Sinon, le service d'intégration n'est pas attribué aux flux de travail déployés.</p> <p>La valeur par défaut est Non.</p>
DEPLOYFOLDER	NEWFOLDERNAME	Facultatif. Crée un dossier avec ce nom.

Élément	Nom de l'attribut	Description de l'attribut
REPLACEFOLDER	FOLDERNAME	Requis si vous utilisez DEPLOYFOLDER. Nom du dossier après l'avoir remplacé.
-	RETAINMAPVARPERVALS	Facultatif. Conserve les valeurs persistantes de la variable de mappage dans la cible.
-	RETAINWFLOWVARPERVALS	Facultatif. Conserve les valeurs persistantes de la variable de flux de travail.
-	RETAINWFLOWSESSLOGS	Facultatif. Conserve les journaux de session de flux de travail dans la cible.
-	MODIFIEDMANUALLY	Facultatif. Compare les dossiers pour vérifier si des objets du dossier cible ont été créés ou modifiés depuis le dernier déploiement.
-	RETAINORIGFOLDEROWNER	Facultatif. Conserve le propriétaire du dossier existant. La commande <i>pmrep</i> ignore les informations fournies dans l'élément DEPLOYEDFOLDEROWNER.
OVERRIDEFOLDER	SOURCEFOLDERNAME	Requis si vous déployez DeployFolder et DeployDeploymentGroup. Si vous déployez un dossier, cet élément spécifie le dossier actuel vers lequel les raccourcis redirigent. Si vous déployez un groupe de déploiement, il spécifie les dossiers suivants : <ul style="list-style-type: none"> - Le ou les dossiers vers lesquels les raccourcis redirigent - Le ou les dossiers contenant les objets du groupe de déploiement
-	SOURCEFOLDERTYPE	Facultatif. Si vous déployez un dossier, cet élément spécifie le type de dossier vers lequel les raccourcis redirigent. Utiliser des raccourcis locaux ou globaux.
-	TARGETFOLDERNAME	Requis. Si vous déployez un dossier, cet élément spécifie le dossier vers lequel les raccourcis redirigent. Si vous déployez un groupe de déploiement, il spécifie les dossiers suivants : <ul style="list-style-type: none"> - Le ou les dossiers vers lesquels les raccourcis redirigent - Le ou les dossiers contenant les objets du groupe de déploiement

Élément	Nom de l'attribut	Description de l'attribut
-	TARGETFOLDERTYPE	Facultatif. Si vous déployez un dossier, cet élément spécifie le type de dossier vers lequel les raccourcis redirigent. Utiliser des raccourcis locaux ou globaux.
-	MODIFIEDMANUALLY	Facultatif. Compare les dossiers pour vérifier si des objets du dossier cible ont été créés ou modifiés depuis le dernier déploiement. Utilisez cet attribut uniquement avec la commande DeployDeploymentGroup.
DEPLOYGROUP	CLEARSRCDPLOYGROUP	Requis si vous utilisez DeployDeploymentGroup. Supprime les objets du groupe source après le déploiement.
-	NEWDEPLOYGROUPNAME	Facultatif. Crée un groupe de déploiement avec ce nom. Ignore si REPLACEDG est spécifié. La valeur par défaut est le nom du groupe de déploiement source.
REPLACEDG	DGNAME	Facultatif. Nom du groupe de déploiement à remplacer.
-	RETAINORIGDGOWNER	Facultatif. Spécifie si vous souhaitez conserver le propriétaire du groupe de déploiement en cours de remplacement dans le référentiel cible.
TARGETDGOWNER	USERNAME	Facultatif. Propriétaire de la copie du groupe de déploiement. La valeur par défaut est le propriétaire du groupe de déploiement source.
-	SECURITYDOMAIN	Facultatif. Domaine de sécurité du groupe de déploiement cible.
APPLYLABEL	SOURCELABELNAME	Requis si vous utilisez DeployDeploymentGroup. Applique un libellé à tous les objets présents dans le groupe source.
-	SOURCEMOVELABEL	Facultatif. Déplace le libellé d'une version différente de l'objet dans le groupe source vers la version de l'objet présente dans le groupe de déploiement. Si l'agent de référentiel détecte que le libellé est appliqué à une autre version du même objet, vous pouvez choisir de déplacer le libellé vers la version de l'objet sélectionné.
-	TARGETLABELNAME	Facultatif. Applique un libellé à tous les objets déployés vers le référentiel cible.

Élément	Nom de l'attribut	Description de l'attribut
-	TARGETMOVELABEL	Facultatif. Déplace le libellé d'une version différente de l'objet dans le groupe cible vers la version de l'objet présente dans le groupe de déploiement. Si l'agent de référentiel détecte que le libellé est appliqué à une autre version du même objet, vous pouvez choisir de déplacer le libellé vers la dernière version de l'objet.
DEPLOYEDFOLDEROWNER	USERNAME	Requis si vous déployez DeployFolder et DeployDeploymentGroup. Propriétaire du dossier déployé ou du groupe de déploiement dans le référentiel cible.
-	SECURITYDOMAIN	Facultatif. Nom du domaine de sécurité auquel le propriétaire du dossier déployé ou du groupe de déploiement appartient.
-	GROUPNAME	Facultatif. Propriétaire de groupe du dossier déployé ou du groupe de déploiement dans le référentiel cible.

Variables de mappage persistantes

Lorsque vous déployez un dossier ou un groupe, vous pouvez copier les valeurs des variables de mappage persistantes du référentiel source vers le référentiel cible, conserver les valeurs du référentiel cible ou les réinitialiser.

Le tableau suivant décrit comment configurer COPYMAPVARPERVALS et RETAINMAPVARPERVALS pour copier, conserver ou réinitialiser les valeurs des variables de mappage persistantes :

Comportement de déploiement	Configuration
Réinitialisez les valeurs des variables de mappage persistantes dans le référentiel cible.	Définissez COPYMAPVARPERVALS sur Non.
Copie les valeurs des variables de mappage du référentiel source vers le référentiel cible.	Définissez les options suivantes du fichier de paramètres : - Définissez COPYMAPVARPERVALS sur Oui. - Définissez RETAINMAPVARPERVALS sur Non.
Conserve les valeurs des variables de mappage persistantes existantes dans le référentiel cible.	Définissez les options suivantes du fichier de paramètres : - Définissez COPYMAPVARPERVALS sur Oui. - Définissez RETAINMAPVARPERVALS sur Oui.

Exemples de fichiers de contrôle de déploiement

Les paramètres que vous spécifiez dans le code du fichier de contrôle de déploiement déterminent les actions qui se produisent lorsque vous exécutez les commandes DeployFolder ou DeployDeploymentGroup dans *pmrep*. Les exemples suivants discutent d'instances dans lesquelles vous utilisez les commandes DeployFolder et DeployDeploymentGroup avec un fichier de contrôle de déploiement.

Déploiement de la dernière version d'un dossier

Vous pouvez déployer la dernière version d'un dossier et inclure toutes les dépendances. Par exemple, vous devez conserver les valeurs actuelles dans une transformation Générateur de séquence et vous devez indiquer les raccourcis de `sc_folder` à `new_sc_folder`. Après avoir copié le dossier, vous souhaitez le renommer « `new_year` ».

Vous pourriez créer un fichier de contrôle avec des attributs suivants :

```
<?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>
```

Déploiement de la dernière version d'un groupe de déploiement

Vous pouvez déployer la dernière version d'un groupe de déploiement et appliquer un libellé aux objets du groupe de déploiement. Par exemple, vous souhaitez appliquer le libellé `NEW_SRC_LABEL_NAME` à tous les objets du groupe source et `NEW_TGT_LABEL_NAME` à tous les objets du groupe cible. Vous pourriez créer un fichier de contrôle avec des attributs suivants :

```
<?xml version="1.0" encoding="UTF-16LE"?>
<!DOCTYPE DEPLOYPARAMS SYSTEM "depctl.dtd">
<DEPLOYPARAMS DEFAULTSERVERNAME="dg_sunqa2_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>
```

Création de liste de plusieurs dossiers source et cible

Utilisez l'élément `OVERRIDEFOLDER` dans le fichier de contrôle pour répertorier plusieurs dossiers source et cible. Utilisez les attributs `SOURCEFOLDERNAME` et `TARGETFOLDERNAME` pour spécifier les dossiers suivants dans les référentiels source et cible :

- Le ou les dossiers vers lesquels les raccourcis redirigent
- Le ou les dossiers contenant les objets du groupe de déploiement

Lorsque vous exécutez la commande *pmrep*, *DeployDeploymentGroup*, le processus de déploiement choisit le dossier cible correct à utiliser après la vérification des objets du groupe de déploiement.

Par exemple, si un groupe de déploiement contient des objets dans deux dossiers avec des raccourcis vers un troisième dossier, vous pouvez créer un fichier de contrôle avec trois occurrences de l'élément *OVERRIDEFOLDER*. L'exemple de fichier de contrôle suivant déploie un groupe de déploiement qui contient des objets dans les dossiers *OBJECTFOLDER1* et *OBJECTFOLDER2* qui eux-mêmes contiennent des raccourcis redirigeant vers le dossier *SHAREDSHORTCUT* :

```
<!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>
```

Conseils d'utilisation de pmrep Files

Utilisez l'option *-n* quand vous utilisez les commandes *pmrep Updatesrcprefix* ou *Updatetargprefix*.

Lorsque vous incluez l'option *-n*, vous devez entrer le nom de l'instance source ou cible pour l'option *-t*. Le nom d'instance source ou cible doit correspondre au nom affiché dans les propriétés de session ou le nom délivré par la commande *Listtablesbyess*.

Utilisez l'option *-n* pour utiliser la commande *Listtablesbyess* avec les commandes *Updatesrcprefix* ou *Updatetargprefix* dans un script shell si les noms des instances source et cible correspondent. En outre, utilisez l'option *-n* pour mettre à jour une source même si la session utilise un raccourci vers un mappage.

Quand vous utilisez la commande *pmrep ListObjects*, entrez un caractère ou un jeu de caractères non utilisés dans des noms d'objet repository pour un séparateur de colonnes, un indicateur de fin d'enregistrement et un indicateur de fin de liste.

Lorsque vous entrez des caractères pour séparer des enregistrements et des colonnes et pour indiquer la fin de la liste, utilisez des caractères qui ne sont pas utilisés dans les noms d'objet repository. Ceci vous aide à utiliser un script shell pour analyser les métadonnées de l'objet.

Dans *pmrep*, utilisez l'option `-v` lorsque vous restaurez un référentiel qui utilise un service de répertoire externe pour la gestion des utilisateurs.

Lorsque vous incluez l'option `-v` l'option avec `Restore`, vous pouvez conserver le service de répertoire externe pour le référentiel. Si vous n'entrez pas cette option avec le nom valide de l'administrateur et son mot de passe, le référentiel restauré se met par défaut en mode d'authentification du référentiel et vous perdez l'association entre les noms de connexion et les noms d'utilisateur.

INDEX

A

- abortAllJobs (infacmd ms) [927](#)
- abortRun (infacmd mi) [831](#)
- aborttask (pmcmd)
 - description [1340](#)
- abortWorkflow
 - infacmd wfs [1188](#)
- AbortWorkflow (pmcmd)
 - description [1342](#)
- AddAlertUser (infacmd isp) [352](#)
- AddConnectionPermissions (infacmd isp) [354](#)
- addCustomLDAPType (infacmd isp)
 - description [356](#)
- AddDomainLink (infacmd isp) [359](#)
- AddDomainNode (infacmd isp) [361](#)
- AddGroupPrivilege (infacmd isp) [363](#), [381](#)
- addLDAPConnectivity (infacmd isp)
 - description [365](#)
- AddLicense (infacmd isp) [368](#)
- AddNamespace (infacmd isp) [370](#)
- AddNodeResource (infacmd isp) [373](#)
- AddParameterSetEntries (infacmd dis) [153](#)
- AddRolePrivilege (infacmd isp) [375](#)
- AddServiceLevel (infacmd isp) [377](#)
- AddToDeploymentGroup (pmrep)
 - description [1387](#)
- AddUserPrivilege (infacmd isp) [379](#)
- Aide (infacmd) [573](#)
- alertes
 - abonner des utilisateurs à [352](#)
 - configuration des paramètres SMTP à l'aide d'infacmd isp [784](#)
 - désabonnement à l'aide d'infacmd isp [664](#)
 - liste des paramètres SMTP à l'aide d'infacmd [643](#)
 - liste des utilisateurs abonnés infacmd isp [581](#)
- application
 - configuration des autorisations pour [226](#)
 - création de la liste des autorisations pour [189](#)
- applications
 - arrêt [236](#)
 - changement de nom [220](#)
 - configuration des propriétés pour [252](#)
 - création de la liste de propriétés pour [187](#)
 - démarrage [235](#)
 - liste d'objets pour [185](#)
 - mise à jour [250](#)
 - purge du cache de l'ensemble des résultats pour [213](#)
 - restauration [224](#)
 - suppression du service d'intégration de données [249](#)
- applications déployées
 - création de liste [190](#)
 - sauvegarde [155](#)
- ApplyLabel (pmrep)
 - description [1389](#)
- AssignDefaultOSProfile (infacmd isp) [383](#)
- AssignedToLicense (infacmd isp) [385](#)

- AssignGroupPermission (infacmd isp) [386](#)
- AssignIntegrationService (pmrep)
 - description [1391](#)
- AssignISToMMService (infacmd isp) [388](#)
- AssignLicense (infacmd isp) [390](#)
- AssignPermission (pmrep)
 - description [1392](#)
- AssignRoleToGroup (infacmd isp) [392](#)
- AssignRoletoUser (infacmd isp) [394](#)
- AssignRSToWSHubService (infacmd isp) [396](#)
- AssignUserPermission (infacmd isp) [398](#)
- authentification LDAP
 - configuration à l'aide d'infacmd isp [356](#), [741](#), [753](#)
- Authentification LDAP
 - configuration à l'aide d'infacmd isp [365](#)
- autorisations
 - assignation à l'aide de pmrep [1392](#)
 - retrait de l'utilisateur ou du groupe des connexions à l'aide d'infacmd isp [668](#)
- autorisations d'utilisateur
 - liste pour les objets de domaine [645](#)
- autorisations de connexion
 - ajout aux utilisateurs ou groupes [354](#)
 - liste à l'aide d'infacmd isp [594](#)
 - liste pour les utilisateurs ou groupes [592](#)
- autorisations du groupe
 - assignation aux objets [386](#)
 - liste pour les objets de domaine [613](#)
 - retrait sur les objets [678](#)
- autotune
 - connexions [85](#)
 - domaine [85](#)
 - services [85](#)

B

- BackupApplication (infacmd dis) [155](#)
- BackupContents (infacmd mrs) [851](#)
- BackupDomain (infasetup)
 - description [1275](#)

C

- cache d'objet de données logique
 - arrêt de l'actualisation [157](#)
- cache de l'objet de données
 - actualisation [218](#)
- cache de la table virtuelle
 - actualisation [1133](#)
 - purge [1131](#)
- CancelDataObjectCacheRefresh (infacmd dis) [157](#)
- cancelProfileExecution (infacmd ps) [962](#)
- cancelWorkflow
 - infacmd wfs [1192](#)

- certificat ADLS
 - mise à jour [99](#)
- chaîne de connexion
 - exemples [1383](#)
 - syntaxe [1383](#)
- ChangeOwner (pmrep)
 - description [1394](#)
- CheckIn (pmrep)
 - description [1395](#)
- CheckInObject (infacmd mrs) [853](#)
- chemin de dossier
 - opérateurs de comparaison [282](#)
- clause Where
 - requête [286](#)
- CleanUp (pmrep)
 - description [1396](#)
- clearConfigurationProperties (cluster infacmd) [108](#)
- ClearDeploymentGroup (pmrep)
 - description [1396](#)
- CloseForceListener (infacmd pwx) [993](#)
- CloseListener (infacmd pwx) [995](#)
- cluster
 - suppression [95](#)
- cluster infacmd
 - actualisation des informations de configuration de cluster [121](#)
 - autorisations d'utilisateur pour une configuration de cluster [120](#)
 - autorisations de groupe sur une configuration de cluster [113](#)
 - création d'une configuration de cluster [101](#), [104](#)
 - effacement des propriétés de configuration [108](#)
 - établissement d'une liste de configurations de cluster [118](#)
 - établissement d'une liste de propriétés de configuration de cluster [116](#)
 - exportation d'une configuration de cluster [110](#)
 - liste des fichiers de configuration de distribution Hadoop [112](#), [115](#)
 - mise à jour des propriétés de configuration [127](#)
 - modification des autorisations de configuration du cluster [123](#)
 - modification des propriétés de configuration de la grappe [125](#)
 - suppression d'objets de configuration [106](#)
- clusters
 - liste [97](#)
- codes de retour
 - infacmd [67](#)
 - infasetup [1274](#)
 - pmcmd [1336](#)
- colonne
 - options pour infacmd [1152](#)
- colonne de table virtuelle
 - configuration des autorisations pour [1136](#)
- colonnes
 - liste des propriétés de [1117](#)
- colonnes virtuelles
 - création de la liste des autorisations pour [1119](#)
 - options de mise à jour [1150](#)
- commandes
 - entrée d'options et d'arguments pour [37](#)
- commandes infacmd
 - obtention d'aide pour [573](#)
- compareMapping
 - infacmd dis [162](#)
- compareObject
 - infacmd dis [166](#)
- completeTask
 - infacmd wfs [1194](#)
- comptes d'utilisateur
 - activation [539](#)
 - désactivation dans un domaine [529](#)
 - édition des propriétés pour [531](#)
- CondenseLogger (infacmd pwx) [998](#)
- configuration
 - utilitaires de ligne de commande [33](#)
- configuration de cluster
 - actualisation [121](#)
 - autorisations de groupe [113](#)
 - création [101](#), [104](#)
 - établissement d'une liste de propriétés [116](#)
 - exportation [110](#)
 - gestion des propriétés [108](#), [127](#)
- configuration de grappe
 - modification [123](#), [125](#)
 - suppression [106](#)
- Configuration du serveur LDAP
 - liste à l'aide d'infacmd isp [632](#)
 - mise à jour à l'aide d'infacmd isp [713](#)
- configurations de cluster
 - autorisations d'utilisateur [120](#)
 - établissement d'une liste [118](#)
 - exportation à l'aide d'infacmd isp [541](#)
 - importation à l'aide d'infacmd isp [574](#)
- Connect (pmcmd)
 - description [1344](#)
- Connect (pmrep)
 - description [1397](#)
- connectivité
 - exemples de chaînes de connexion [1383](#)
- connexion
 - Web Content-Kapow Katalyst [478](#)
- Connexion Confluent Kafka
 - créer avec infacmd [417](#)
- Connexion de stockage Blob Microsoft Azure
 - propriétés infacmd [451](#)
- Connexion LDAP
 - liste à l'aide d'infacmd isp [583](#), [586](#), [601](#), [618](#), [670](#), [682](#)
- Connexion Microsoft Azure Data Lake Storage Gen1
 - propriétés infacmd [452](#)
- Connexion Microsoft Azure Data Lake Storage Gen2
 - propriétés infacmd [452](#)
- Connexion Microsoft Azure SQL Data Warehouse
 - propriétés infacmd [453](#)
- Connexion Teradata Parallel Transporter
 - infacmd [473](#)
- connexions
 - création avec la commande infacmd [402](#)
 - exportation à l'aide d'infacmd isp [541](#)
 - importation à l'aide d'infacmd isp [574](#)
 - liste à l'aide d'infacmd isp [598](#)
 - liste des options pour l'utilisation d'infacmd isp [590](#), [600](#)
 - mise à jour à l'aide d'infacmd isp [737](#)
 - modification d'un nom avec la commande infacmd [705](#)
 - Oracle [462](#)
 - retrait des domaines à l'aide d'infacmd isp [666](#)
- Connexions HBase pour MapR-DB
 - propriétés infacmd [451](#)
- content
 - importation depuis des fichiers d'application [1072](#)
- contenu de l'entrepôt de profilage
 - retrait [967](#)
- ConvertLogFile (infacmd isp) [400](#)
- correctif
 - application [1185](#)
 - application incrémentielle [1185](#)
- Create (pmrep)
 - description [1399](#)
- CreateAuditTables (infacmd cms) [130](#)
- createConfiguration (cluster infacmd) [101](#), [104](#)
- CreateConnection (infacmd isp) [402](#)

[CreateConnection \(pmrep\)](#)
 description [1400](#)
[CreateContent \(infacmd tdm\)](#) [1166](#)
[CreateContents \(infacmd mrs\)](#) [855](#)
[createdatamaps \(infacmd pwx\)](#) [1000](#)
[CreateDeploymentGroup \(pmrep\)](#)
 description [1403](#)
[CreateExceptionAuditTables \(infacmd comme\)](#) [68](#)
[CreateFolder \(infacmd isp\)](#) [479](#)
[CreateFolder \(pmrep\)](#)
 description [1404](#)
[CreateGrid \(infacmd isp\)](#) [480](#)
[CreateGroup \(infacmd isp\)](#) [482](#)
[CreateGroup \(pmrep\)](#)
 description [1406](#)
[CreateIntegrationService \(infacmd isp\)](#) [484](#)
[CreateLabel \(pmrep\)](#)
 description [1406](#)
[CreateListenerService \(infacmd pwx\)](#) [1003](#)
[CreateLoggerService \(infacmd pwx\)](#) [1006](#)
[CreateMMSservice \(infacmd isp\)](#) [494](#)
[CreateOSProfile \(infacmd isp\)](#) [498](#)
[CreateProject \(infacmd mrs\)](#) [857](#), [858](#)
[CreateRepositoryService \(infacmd isp\)](#) [504](#)
[CreateRole \(infacmd isp\)](#) [509](#)
[CreateSAPBWService \(infacmd isp\)](#) [510](#)
[CreateSchedule \(infacmd sch\)](#) [1080](#)
[CreateService \(infacmd cms\)](#) [132](#)
[CreateService \(infacmd comme\)](#) [70](#)
[CreateService \(infacmd dis\)](#) [159](#)
[CreateService \(infacmd edp\)](#) [303](#)
[CreateService \(infacmd idp\)](#) [293](#)
[CreateService \(infacmd mas\)](#) [817](#)
[CreateService \(infacmd mi\)](#) [833](#)
[CreateService \(infacmd mrs\)](#) [860](#)
[CreateService \(infacmd search\)](#) [1105](#)
[CreateService \(infacmd tdm\)](#) [1159](#)
[CreateUser \(infacmd isp\)](#) [514](#)
[CreateWH \(infacmd ps\)](#) [964](#)
[CreateWSHubService \(infacmd isp\)](#) [517](#)

D

DB2
 options de connexion infacmd [438](#)
[DefineDomain \(infasetup\)](#)
 description [1278](#)
[DefineGatewayNode \(infasetup\)](#)
 description [1288](#)
[DefineWorkerNode \(infasetup\)](#)
 description [1294](#)
[delegateTask](#)
 infacmd wfs [1198](#)
[Delete \(pmrep\)](#)
 description [1412](#)
[DeleteauditHistory \(infacmd bg\)](#) [88](#)
[DeleteAuditTables \(infacmd cms\)](#) [134](#)
[deleteClusters \(infacmd ccps\)](#) [95](#)
[deleteConfiguration \(grappe infacmd\)](#) [106](#)
[DeleteConnection \(pmrep\)](#)
 description [1413](#)
[DeleteContents \(infacmd mrs\)](#) [864](#)
[DeleteDeploymentGroup \(pmrep\)](#)
 description [1414](#)
[DeleteDomain \(infasetup\)](#)
 description [1298](#)
[DeleteExceptionAuditTables \(infacmd as\)](#) [72](#)

[DeleteFolder \(infacmd mrs\)](#) [866](#)
[DeleteFolder \(pmrep\)](#)
 description [1414](#)
[DeleteLabel \(pmrep\)](#)
 description [1414](#)
[deleteMappignPersistedOutputs](#)
 infacmd ms [929](#)
[DeleteNamespace \(infacmd isp\)](#) [521](#)
[DeleteObject \(pmrep\)](#)
 description [1415](#)
[DeleteParameterSetEntries \(infacmd dis\)](#) [170](#), [198](#)
[DeleteProject \(infacmd mrs\)](#) [868](#)
[DeleteSchedule \(infacmd sch\)](#) [1087](#)
[depcntl.dtd](#)
 création de liste [1501](#)
[déploiement des objets](#)
 depcntl.dtd [1501](#)
[DeployApplication \(infacmd dis\)](#) [176](#)
[DeployDeploymentGroup \(pmrep\)](#)
 description [1416](#)
[déployer](#)
 correctif [1185](#)
[DeployFolder \(pmrep\)](#)
 description [1418](#)
[DeployImport \(infacmd rtm\)](#) [1072](#)
[deployObjects](#)
 infacmd tools [1172](#)
[deployObjectsToFile](#)
 infacmd dis [172](#)
[deploySpec \(infacmd mi\)](#) [837](#)
 description [659](#)
[detectOrphanResults \(infacmd ps\)](#) [966](#)
[DétruireConnexionUtilisateur \(pmrep\)](#)
 description [1427](#)
[déverrouillage](#)
 objet verrouillé [911](#)
[DisableNodeResource \(infacmd isp\)](#) [523](#)
[DisableService \(infacmd isp\)](#) [525](#)
[DisableService \(infacmd tdm\)](#) [1169](#)
[DisableServiceProcess \(infacmd isp\)](#) [527](#)
[DisableUser \(infacmd isp\)](#) [529](#)
[Disconnect \(pmcmd\)](#)
 description [1345](#)
[DisplayAllLogger \(infacmd pwx\)](#) [1010](#)
[DisplayCPULogger \(infacmd pwx\)](#) [1013](#)
[DisplayEventsLogger \(infacmd pwx\)](#) [1015](#)
[DisplayMemoryLogger \(infacmd pwx\)](#) [1018](#)
[DisplayRecordsLogger \(infacmd pwx\)](#) [1021](#)
[displayStatsListener \(infacmd pwx\)](#) [1024](#)
[DisplayStatusLogger \(infacmd pwx\)](#) [1027](#)
[domaine multiversions](#)
 exécuter pmrep [1382](#)
 exécution de pmcmd [1335](#)
[domaines](#)
 création à l'aide de la commande infasetup [1278](#)
 liste des domaines liés à l'aide d'infacmd isp [607](#)
 liste des propriétés à l'aide d'infacmd isp [608](#)
 mise à jour avec la commande infasetup [1311](#)
 mise à jour des propriétés à l'aide d'infacmd isp [744](#)
 ping [656](#)
 restauration à l'aide de la commande infasetup [1303](#)
 sauvegarde à l'aide de la commande infasetup [1275](#)
 suppression de liens à l'aide d'infacmd isp [672](#)
 suppression en utilisant la commande infasetup [1298](#)
[domaines de sécurité](#)
 liste à l'aide d'infacmd [635](#)
[données de processus de flux de travail](#)
 suppression de la base de données [1212](#)

dossiers
 création dans un domaine [479](#)
 déplacement à l'aide d'infacmd isp [652](#)
 déplacement d'objets entre à l'aide d'infacmd isp [654](#)
 déploiement [1418](#)
 liste à l'aide d'infacmd isp [610](#)
 mise à jour de la description à l'aide d'infacmd isp [746](#)
 modification [1444](#)
 retrait à l'aide d'infacmd isp [674](#)
 suppression [1414](#)
dropTables (infacmd wfs) [1200](#)
DropWH (infacmd ps) [967](#)

E

EditUser (infacmd isp) [531](#)
EditUser (pmrep)
 description [1419](#)
EnableNodeResource (infacmd isp) [534](#)
EnableService (infacmd isp) [535](#)
EnableService (infacmd tdm) [1168](#)
EnableServiceProcess (infacmd isp) [537](#)
EnableUser (infacmd isp) [539](#)
événements du journal
 purge à l'aide d'infacmd isp [660](#)
 troncation à l'aide de pmrep [1459](#)
Execute (infacmd ps) [969](#)
executeProfile (infacmd ps) [971](#)
ExecuteQuery (pmrep)
 description [1419](#)
exécuter le résumé
 déploiement de mi spec [842](#)
ExecuteSQL (infacmd sql) [1117](#)
exécution d'un mappage
 avec un ensemble de paramètres d'exécution [947](#)
Exit (pmrep)
 description [1421](#)
Export (infacmd rtm) [1074](#)
exportConfiguration (cluster infacmd) [110](#)
exportControl.xsd
 fichiers de contrôle infacmd [1256](#)
ExportDomainObjects (infacmd isp)
 description [541](#)
exportGlossary (infacmd bg) [90](#)
exportObjects
 infacmd tools [1174](#)
exportResources
 infacmd tools [1177](#)
exportSpec
 infacmd mi [838](#)
ExportToPC (infacmd ipc) [342](#)
ExportUsersAndGroups (infacmd isp) [544](#)

F

fiches d'évaluation
 exécution [969](#)
 liste les résultats de [977](#)
 migration [982](#)
 purge les résultats de [984](#)
fichier d'entrée persistant
 création avec pmrep [1488](#)
fichier de contrôle
 déploiement [1501](#)
 Exemple ObjectImport XML [1494](#)
 importez un objet [1490](#)

fichier de contrôle de déploiement
 description [1501](#)
fichier de contrôle de l'importation d'objet
 description [1490](#)
fichier DTD
 plug-in modèle [1454](#)
fichier XML
 plug-in modèles [1454](#)
fichiers archive d'application (iar) de fichiers
 déploiement sur le service d'intégration de données [176](#)
fichiers de contrôle
 conventions de nommage [1256](#)
 exemples d'objets du référentiel modèle [1271](#)
 exemples pour les objets de domaine [1270](#)
 fichiers de schéma [1256](#)
 infacmd [1255](#)
 paramètres pour les objets de domaine [1257](#), [1262](#)
 paramètres pour les objets du référentiel modèle [1259](#), [1264](#)
 règles et instructions [1269](#)
fichiers de contrôle d'exportation
 conventions de nommage [1256](#)
 exemples d'objets du référentiel modèle [1271](#)
 exemples pour les objets de domaine [1270](#)
 fichiers de schéma [1256](#)
 infacmd [1255](#)
 paramètres pour les objets de domaine [1257](#)
 paramètres pour les objets du référentiel modèle [1259](#)
 règles et instructions [1269](#)
fichiers de contrôle d'importation
 conventions de nommage [1256](#)
 exemples d'objets du référentiel modèle [1271](#)
 exemples pour les objets de domaine [1270](#)
 fichiers de schéma [1256](#)
 infacmd [1255](#)
 paramètres pour les objets de domaine [1262](#)
 paramètres pour les objets du référentiel modèle [1264](#)
 règles et instructions [1269](#)
fichiers de paramètres
 utilisation avec pmcmd StartTask [1366](#)
 utilisation avec pmcmd StartWorkflow [1369](#)
fichiers de paramètres locaux
 utilisation avec pmcmd StartWorkflow [1369](#)
fichiers de schéma
 fichiers de contrôle infacmd [1256](#)
fichiers journaux binaires
 conversion en texte, XML ou en texte lisible à l'écran [400](#)
fichiers script
 exécution [1457](#)
 utilisation pour commandes pmrep [1384](#)
FileSwitchLogger (infacmd pwx) [1030](#)
FindCheckout (pmrep)
 description [1421](#)
flux de travail
 arrêt à partir de la ligne de commande [1372](#)
 configuration des autorisations pour [228](#)
 création d'une liste [1211](#)
 démarrage à partir de la ligne de commande [1367](#)
 obtention d'événements du journal pour [570](#)
 récupération à l'aide de la syntaxe pmcmd [1359](#)
flux de travail déployés sur le service d'intégration de données
 abandon [1188](#)
 annulation [1192](#)
 démarrage [1222](#)
 récupération [1214](#)
flux de travail simultanés
 arrêt à partir de la ligne de commande [1372](#)
 démarrage à partir de la ligne de commande [1367](#)

fonctions
validation [790](#)
fuseau horaire Olson
valeurs valides [1083](#)
fuseaux horaires
valeurs valides pour la planification [1083](#)

G

GenerateAbapProgramToFile (pmrep)
description [1423](#)
GenerateEncryptionKey (infasetup)
description [1301](#)
generateReadableViewXML
infacmd xrf [1253](#)
genreuserreportfrompc (infacmd ipc) [348](#)
Getconnectiondetails (pmrep)
description [1423](#)
getDomainObjectPermissions (infacmd aud) [77](#)
getExecutionStatus (infacmd ps) [973](#)
GetFolderInfo (infacmd isp) [546](#)
GetLastError (infacmd isp) [548](#)
GetLog (infacmd isp) [550](#)
GetMappingStatus
infacmd ms [933](#)
GetNodeName (infacmd isp) [553](#)
GetPasswordComplexityConfig (infacmd) [554](#)
getPrivilegeAssociation (infacmd aud) [78](#)
getProfileExecutionStatus (infacmd ps) [975](#)
GetRequestLog
infacmd ms [935](#)
getrunningsessionsdetails (pmcmd)
description [1346](#)
getSamlConfig (infacmd)
description [555](#)
GetServiceDetails (pmcmd)
description [1347](#)
GetServiceOption (infacmd isp) [557](#)
GetServiceProcessOption (infacmd isp) [558](#)
GetServiceProcessStatus (infacmd isp) [560](#)
getserviceproperties (pmcmd)
description [1349](#)
GetServiceStatus (infacmd isp) [562](#)
GetSessionLog (infacmd isp) [563](#)
GetSessionStatistics (pmcmd)
description [1350](#)
getSpecRunStats
infacmd mi [841](#)
GetSystemLogDirectory (infacmd isp) [567](#)
gettaskdetails (pmcmd)
description [1352](#)
getUserGroupAssociation (infacmd aud) [80](#), [81](#)
getUsersPersonalInfo (infacmd aud) [82](#)
getworkflowdetails (pmcmd)
description [1354](#)
GetWorkflowLog (infacmd isp) [570](#)
grilles
création [480](#)
liste de nœuds à l'aide d'infacmd isp [611](#)
mise à jour des nœuds assignés à l'aide d'infacmd isp [749](#)
retrait à l'aide d'infacmd isp [675](#)
groupes
création dans les domaines [482](#)
exportation [544](#)
exportation à l'aide d'infacmd isp [541](#)
importation à l'aide d'infacmd isp [574](#), [579](#)
liste à l'aide d'infacmd isp [584](#)

groupes (*a continué*)
liste pour un utilisateur [616](#)
retrait à l'aide d'infacmd isp [677](#)
groupes de déploiement
création de la liste de plusieurs dossiers [1508](#)

H

help (pmcmd)
description [1357](#)
Help (pmrep)
description [1425](#)
hôtes de passerelle du domaine
ping [656](#)
Hub de services Web
association d'un référentiel à l'aide d'infacmd isp [396](#)
création dans un domaine [517](#)
dissociation d'un référentiel à l'aide d'infacmd isp [734](#)
mise à jour à l'aide d'infacmd isp [786](#)

I

IBM DB2
exemple de chaîne de connexion [1383](#)
ICMD_JAVA_OPTS
configuration [46](#)
impcntl.dtd
description [1490](#)
Import (infacmd rtm) [1077](#)
importation d'objets
Exemple ObjectImport XML [1494](#)
impcntl.dtd [1490](#)
importControl.xsd
fichiers de contrôle infacmd [1256](#)
ImportDomainObjects (infacmd isp)
description [574](#)
importer depuis PowerCenter
options [346](#)
importGlossary (infacmd bg) [92](#)
importObjects
infacmd tools [1179](#)
ImportUsersAndGroups (infacmd isp)
description [579](#)
INFA_CLIENT_RESILIENCE_TIMEOUT
configuration [46](#)
INFA_CODEPAGENAME
configuration [47](#)
INFA_DEFAULT_DATABASE_PASSWORD
configuration [48](#)
INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD
configuration [49](#)
INFA_DEFAULT_DOMAIN
configuration [50](#)
INFA_DEFAULT_DOMAIN_PASSWORD
configuration [50](#)
INFA_DEFAULT_DOMAIN_USER
configuration [51](#)
INFA_DEFAULT_PWX_OSEPASSWORD
configuration [52](#)
INFA_DEFAULT_PWX_OSPASSWORD
configuration [53](#)
INFA_JAVA_CMD_OPTS
configuration [55](#)
INFA_NODE_KEYSTORE_PASSWORD
configuration [57](#)

INFA_NODE_TRUSTSTORE_PASSWORD

configuration [58](#)

INFA_PASSWORD

configuration [55](#)

INFA_REPCNX_INFO

configuration [58](#)

INFA_REPOSITORY_PASSWORD

configuration [59](#)

infacmd

affichage de l'aide pour les commandes [573](#)

codes de retour [67](#)

dissociation du service de gestionnaire de métadonnées [726](#)

domaines de sécurité, liste [635](#)

exécution de commandes [65](#)

fichiers de contrôle [1255](#)

informations de version, affichage [792](#)

licences, annulation de l'assignation [728](#)

liste des identifiants de plug-in pour [65](#)

nœuds, basculement de travail à passerelle [719](#)

Option de processus du service SAP BW [514](#)

options de processus de service [492](#)

Options du Hub de services Web [520](#)

Options du service d'intégration [488](#), [915](#)

Options du service SAP BW [513](#)

répertoire les utilisateurs avec mot de passe faible [649](#)

vérification du statut de la complexité du mot de passe [554](#)

infacmd advanced

validation de fonctions [790](#)

infacmd as

liste de configuration pour le service Analyst [73](#)

mise à jour des propriétés du service Analyst [74](#)

suppression des tables d'audit d'exception [72](#)

infacmd autotune

Autotune [85](#)

infacmd bg

Exportation des glossaires d'entreprise à partir de l'outil Analyst tool [90](#)

Importation de glossaires d'entreprise à partir de fichiers .xlsx ou .zip vers l'outil Analyst tool [92](#)

liste des glossaires d'entreprise dans l'outil Analyst tool [89](#)

Mise à niveau des données de Business Glossary dans le référentiel modèle [87](#)

Suppression de l'historique de l'audit d'un glossaire de l'outil Analyst tool [88](#)

infacmd ccps

liste des clusters [97](#)

mettre à jour le certificat principal de service ADLS [99](#)

supprimer des clusters [95](#)

infacmd cms

configuration des options de processus de service de gestion du contenu [148](#)

création d'un service de gestion de contenu dans un domaine [132](#)

création d'une liste d'options de processus de service de gestion du contenu [138](#)

création de la liste des options pour le service de gestion du contenu [136](#)

création des tables de suivi d'audit [130](#)

mise à jour des options pour le service de gestion du contenu [145](#)

mise à niveau de service [150](#)

purge des données de référence orphelines [139](#)

retrait d'un service de gestion du contenu d'un domaine [141](#)

suppression des tables de suivi d'audit [134](#)

synchronisation des données [143](#)

infacmd comme

configuration des propriétés du processus de service Analyst [75](#)

création d'un service Analyst dans un domaine [70](#)

création de tables d'audit pour les exceptions [68](#)

liste des propriétés du processus du service Analyst [73](#)

infacmd dis

actualisation du cache de l'objet de données [218](#)

ajout d'entrées d'ensemble de paramètres [153](#)

arrêt d'applications [236](#)

arrêt de l'actualisation du cache d'objet de données logique [157](#)

arrêt du service Blaze [238](#)

changement du nom des applications déployées [220](#)

compareMapping [162](#)

compareObject [166](#)

configuration des autorisations d'application [226](#)

configuration des autorisations d'objet d'application [228](#)

configuration des propriétés d'un processus de service d'intégration de données [275](#)

configuration des propriétés de calcul [254](#)

configuration des propriétés de l'application [252](#)

configuration des propriétés de l'objet de données [256](#)

configuration des propriétés du service d'intégration de données [261](#)

création d'un service d'intégration de données [159](#)

définition des autorisations de flux de travail [228](#)

définition des autorisations de mappage [228](#)

démarrage des applications [235](#)

déploiement des fichiers archive d'application (iar) [176](#)

deployObjectsToFile [172](#)

instructions pour CI/CD [278](#)

liste d'objets d'un ensemble de paramètres [200](#)

liste d'objets pour les applications [185](#)

liste des applications déployées [190](#)

liste des autorisations d'application [189](#)

Liste des autorisations d'objet d'application des utilisateurs ou des groupes [183](#)

liste des objets de séquence [206](#)

liste des propriétés d'un processus de service d'intégration de données [210](#)

liste des propriétés de calcul [192](#)

liste des propriétés des applications [187](#)

liste des propriétés des objets de séquence [204](#)

liste des propriétés du service d'intégration des données [208](#)

listPatchNames [203](#)

mise à jour d'applications [250](#)

mise à jour de la valeur actuelle pour l'objet de données de séquence [232](#)

mise à jour des entrées d'ensemble de paramètres [259](#)

options des objets de données [258](#)

purge du cache de l'ensemble des résultats [213](#)

purge du cache pour les objets de données logiques [211](#)

queryDesignTimeObjects [215](#)

queryRunTimeObjects [217](#)

répertoire des propriétés des objets de données [193](#)

répertoire les ensembles de paramètres dans une application [201](#)

répertorier les mappages

dans le DIS [195](#)

dans le service d'intégration de données [195](#)

replaceAllTag [246](#)

requête [280](#)

restauration d'applications à partir de fichiers de sauvegarde [224](#)

sauvegarde de l'application déployée [155](#)

suppression d'entrées d'ensemble de paramètres [170](#), [198](#)

suppression des applications [249](#)

tag [241](#)

untag [243](#)

infacmd edp

création du service Enterprise Data Preparation... [303](#)

mise à jour du service Enterprise Data Preparation [310](#)

mise à niveau du service Enterprise Data Preparation [313](#)

purge des événements d'audit d'Enterprise Data Preparation [307](#)

infacmd idp

création du service de préparation de données interactive [293](#)

infacmd idp (*a continué*)
 mise à jour du service de préparation de données interactive [297](#)

infacmd ipc
 exportation d'objets depuis le référentiel modèle [342](#)
 objet de rapport, réutilisation [348](#)

infacmd isp
 abonner des utilisateurs aux notifications [352](#)
 activation de processus de service sur un nœud [537](#)
 activation de services d'applications [535](#)
 activation des comptes utilisateur [539](#)
 activation des ressources [534](#)
 affichage des listes de configurations de suites de chiffres [604](#)
 ajout d'un lien de domaine [359](#)
 ajout d'utilisateurs aux groupes dans un domaine [381](#)
 ajout de licences de domaines [368](#)
 ajout de niveaux de service [377](#)
 ajout de nœuds à un domaine [361](#)
 ajout de ressources aux nœuds [373](#)
 alertes, configuration des paramètres SMTP [784](#)
 alertes, désabonnement de [664](#)
 alertes, liste des utilisateurs abonnés [581](#)
 assignation d'autorisations de connexion aux utilisateurs ou groupes [354](#)
 assignation de privilèges à des groupes [363](#)
 assignation de privilèges à des utilisateurs [379](#)
 assignation de rôle aux groupes de domaines ou services d'applications [392](#)
 assignation de rôles aux utilisateurs [394](#)
 assignation des licences au service d'application [390](#)
 assignation du service d'intégration [388](#)
 assigner des privilèges à des rôles dans des groupes [375](#)
 association d'un référentiel au Hub de services Web [396](#)
 attribution d'autorisations d'utilisateur sur les objets [398](#)
 attribution d'autorisations du groupe aux objets [386](#)
 attribution de profil de système d'exploitation par défaut [383](#)
 authentification LDAP, configuration [356](#), [741](#), [753](#)
 Authentification LDAP, configuration [365](#)
 autorisations de connexion, liste par groupe [594](#)
 autorisations, suppression des connexions d'utilisateurs ou de groupes [668](#)
 Configuration du serveur LDAP, liste [632](#)
 Configuration du serveur LDAP, mise à jour [713](#)
 configurations de cluster, exportation [541](#)
 configurations de grappe, importation [574](#)
 connexions, exportation [541](#)
 connexions, importation [574](#)
 connexions, liste [598](#)
 connexions, liste d'options pour [590](#), [600](#)
 connexions, mise à jour des propriétés [737](#)
 connexions, retrait des domaines [666](#)
 conversion de fichiers journaux binaires [400](#)
 création d'un service d'intégration dans un domaine [484](#)
 création d'un service de gestionnaire de métadonnées dans un domaine [494](#)
 création d'un service de référentiel dans un domaine [504](#)
 création d'un service Hub de services Web dans le domaine [517](#)
 création d'utilisateurs dans un domaine [514](#)
 création de dossiers [479](#)
 création de grilles [480](#)
 création de groupes dans les domaines [482](#)
 création de la connexion [402](#)
 création de profils de système d'exploitation dans un domaine [498](#)
 création de rôles dans un domaine [509](#)
 création de service SAP BW dans un domaine [510](#)
 désactivation de services d'application [525](#)
 désactivation des comptes utilisateur [529](#)
 désactivation des processus de service sur un nœud [527](#)
 désactivation des ressources de PowerCenter [523](#)

infacmd isp (*a continué*)
 domaine de ping [657](#)
 domaines, liste des domaines liés [607](#)
 domaines, liste des propriétés [608](#)
 domaines, mise à jour des propriétés [744](#)
 domaines, retrait des liens [672](#)
 dossiers, déplacement [652](#)
 dossiers, déplacement d'objets entre [654](#)
 dossiers, liste [610](#)
 dossiers, mise à jour de la description [746](#)
 dossiers, retrait [674](#)
 édition des propriétés de compte utilisateur [531](#)
 événements du journal, purge [660](#)
 exportation d'utilisateurs et de groupes vers un fichier [544](#)
 fichiers de contrôle d'exportation [1257](#)
 fichiers de contrôle d'importation [1261](#)
 grilles, liste de nœuds [611](#)
 grilles, mise à jour des nœuds assignés [749](#)
 grilles, retrait [675](#)
 groupes, liste [584](#)
 groupes, liste de privilèges pour [615](#)
 groupes, retrait [677](#)
 groupes, retrait des privilèges de [680](#)
 Hub de services Web, dissociation d'un référentiel [734](#)
 Hub de services Web, mise à jour [786](#)
 informations de passerelle, mise à jour [748](#)
 LDAP, connexion, liste [583](#), [586](#), [601](#), [618](#), [670](#), [682](#)
 licences, affichage d'informations [716](#)
 licences, liste [620](#)
 licences, mise à jour [756](#)
 licences, retrait [684](#)
 liste d'utilisateurs avec des autorisations pour une connexion [596](#)
 liste de rôles de nœud [626](#)
 liste des objets de domaine pour le groupe [613](#)
 liste des objets de domaine pour les utilisateurs [645](#)
 liste des paramètres SMTP pour le serveur de messagerie sortante [643](#)
 liste des profils de système d'exploitation par défaut [603](#)
 liste des propriétés de dossiers [546](#)
 listes des autorisations des utilisateurs ou groupes pour une connexion [592](#)
 migration des utilisateurs [650](#)
 mise à jour du rôle du nœud [768](#)
 mots de passe, réinitialisation des mots de passe utilisateur [707](#)
 niveaux de service, liste [636](#)
 niveaux de service, mise à jour [781](#)
 niveaux de service, retrait [696](#)
 nœuds, basculement de passerelle à travail [721](#)
 nœuds, dissociation des domaines [735](#)
 nœuds, fermeture [717](#)
 nœuds, liste [628](#), [638](#)
 nœuds, liste des options [623](#)
 nœuds, mise à jour [766](#)
 nœuds, retrait [686](#)
 obtention d'événements de journaux spécifié [550](#)
 obtention d'événements du journal pour les flux de travail [570](#)
 obtention d'une propriété du processus de service d'intégration [558](#)
 obtention des événements du journal pour les sessions [563](#)
 obtention des messages d'erreur récents [548](#)
 obtention des noms de nœud [553](#)
 obtention des propriétés de service [557](#)
 obtention du chemin de référentiel de journal système [567](#)
 obtention du statut d'un service d'application [562](#)
 obtention du statut du processus de service d'application sur un nœud [560](#)
 ping sur objets [656](#)
 processus de service, mise à jour [782](#)
 profil de système d'exploitation, mise à jour [771](#)

infacmd isp (a continué)

- profil du processeur, calcul [709](#)
- profil du système d'exploitation, liste [630](#)
- profil du système d'exploitation, retrait [689](#)
- Propriétés du service de gestionnaire de métadonnées, mise à jour [758](#)
- renommer la connexion [705](#)
- répertoire des groupes pour un utilisateur [616](#)
- répertoire les services assignés à une licence [385](#)
- ressources, liste pour les nœuds [625](#)
- ressources, retrait des nœuds [687](#)
- retirer les autorisations d'utilisateur sur des objets [700](#)
- retrait des autorisations du groupe sur les objets [678](#)
- retrait des autorisations pour utilisateurs et groupes [711](#)
- rôles, exportation [541](#)
- rôles, importation [574](#)
- rôles, liste des privilèges pour [633](#)
- rôles, listes [587](#)
- rôles, retirer à l'utilisateur [731](#)
- rôles, retrait [691](#)
- rôles, retrait des privilèges des [692](#)
- rôles, suppression d'un groupe [730](#)
- Services d'intégration, mise à jour [751](#)
- Services de référentiel, mise à jour [774](#)
- Services SAP BW, mise à jour [779](#)
- services, liste [641](#)
- services, liste des privilèges pour [639](#)
- services, retrait [694](#)
- suppression du profil de système d'exploitation par défaut [725](#)
- synchronisation des utilisateurs et des groupes dans le domaine de sécurité avec des utilisateurs et des groupes LDAP [723](#)
- utilisateurs et groupes, exportation [541](#)
- utilisateurs et groupes, importation [574](#), [579](#)
- utilisateurs, liste des privilèges pour [647](#)
- utilisateurs, listes [589](#)
- utilisateurs, retrait [697](#)
- utilisateurs, retrait d'un groupe [699](#)
- utilisateurs, retrait de privilèges de [703](#)

infacmd mas

- configuration des propriétés de processus de service d'accès aux métadonnées [828](#)
- configuration des propriétés du service d'accès aux métadonnées [825](#)
- création d'un service d'accès aux métadonnées [817](#)
- liste des propriétés de processus de service d'accès aux métadonnées [823](#)
- liste des propriétés du service d'accès aux métadonnées [821](#)

infacmd mi

- abandon d'une spécification d'ingestion de masse [831](#)
- création du service d'ingestion de masse [833](#)
- déploiement de la spécification d'ingestion de masse [837](#)
- déploiement de spéc [838](#)
- extendedRunStats [839](#)
- liste de mi specs [843](#)
- listSpecRuns [842](#)
- obtention des stats de spéc [841](#)
- redémarrage de tâches [844](#)
- running mi spec [845](#)

infacmd mrs

- archivage d'objets [853](#)
- création d'un projet [857](#), [858](#)
- création du contenu du référentiel pour un service de référentiel modèle [855](#)
- création du service de référentiel modèle [860](#)
- déverrouillage d'un objet [911](#)
- gestion des autorisations de groupe sur le projet [891](#)
- gestion des autorisations utilisateur sur le projet [893](#)

infacmd mrs (a continué)

- Liste de dossiers dans le référentiel du service de référentiel modèle [878](#)
- Liste des autorisations dans plusieurs projets [884](#)
- Liste des fichiers du dossier de sauvegarde [875](#)
- liste des objets extraits [876](#)
- liste des objets verrouillés [880](#)
- liste des options du processus de service de référentiel modèle [889](#)
- Liste des options du service de référentiel modèle [888](#)
- Liste des projets dans le référentiel du service de référentiel modèle [886](#)
- Mise à jour des options du processus de service pour le Service de Référentiel Modèle [920](#)
- Mise à jour des options du service de référentiel modèle [913](#)
- Mise à jour des statistiques du service de référentiel modèle [921](#)
- mise à niveau du Service de Référentiel Modèle [923](#)
- réattribution de l'objet extrait [896](#)
- réattribution de l'objet verrouillé [896](#)
- régénération du graphique de dépendance d'objet [898](#)
- remplissage du système de contrôle de version [895](#)
- renommer un dossier [900](#)
- répertorier les mappages du service de référentiel modèle [882](#)
- restauration du contenu du référentiel modèle [903](#)
- rétablissement d'objets extraits [905](#), [909](#)
- sauvegarde du contenu du référentiel modèle dans un fichier [851](#)
- suppression d'un dossier [866](#)
- suppression d'un projet [868](#)
- suppression du contenu du référentiel modèle [864](#)

infacmd ms

- abandon des tâches du service d'intégration de données [927](#)
- création de liste de mappages dans une application [943](#)
- écriture du journal de mappage [935](#)
- exécution d'un mappage déployé sur le service d'intégration de données [947](#)
- mise à jour des options de mappage dans une application [952](#)
- mise à jour du niveau d'optimisation dans une application ou dans un mappage [956](#)
- mise à jour du niveau d'optimisation par défaut dans une application ou un mappage [954](#)
- mise à niveau du fichier de paramètres de mappage [958](#)
- obtention du statut de mappage [933](#)
- purge des lignes de la table de tâches de la base de données [945](#)
- recupérer les journaux de cluster agrégés [931](#)
- répertorier les options de mappage dans une application [937](#)
- suppression des sorties de mappage persistantes [929](#)

infacmd oie

- fichiers de contrôle d'exportation [1257](#)
- fichiers de contrôle d'importation [1261](#)

infacmd ps

- création d'un entrepôt de profilage de données [964](#)
- exécution d'un modèle de profil [971](#)
- exécution des résultats du profil et de la fiche d'évaluation [969](#)
- liste des résultats du profil et de la fiche d'évaluation [977](#)
- migration de clés [990](#)
- migration des résultats de profil [980](#)
- migration résultats des fiches d'évaluation [982](#)
- modèle de profil Gcenceling [962](#)
- obtention du statut de la tâche du profil [973](#)
- obtention du statut du modèle de profil [975](#)
- purge les résultats du profil et de la fiche d'évaluation [984](#)
- suppression du contenu de l'entrepôt de profilage [967](#)

infacmd pwx

- affichage de l'état de la sous-tâche du programme d'écriture du service de journalisation [1027](#)
- affichage de l'utilisation de la mémoire pour le service de journalisation [1018](#)
- affichage de tous les messages du service de journalisation [1010](#)
- affichage des événements du service de journalisation [1015](#)

infacmd pwx (a continué)

- affichage des informations concernant les tâches actives du service d'écoute [1032](#)
- affichage des informations CPU du service de journalisation [1013](#)
- affichage des statistiques de surveillance pour le service d'écoute et ses tâches [1024](#)
- affichage du nombre d'enregistrements de modifications traités par le service de journalisation [1021](#)
- arrêt des tâches du service d'écoute [1038](#)
- arrêt du service d'écoute [995](#)
- arrêt du service de journalisation [1035](#)
- arrêt forcé du service d'écoute [993](#)
- basculement à un nouvel ensemble de fichiers journaux du service de journalisation [1030](#)
- création d'un service d'écoute [1003](#)
- création d'un service de journalisation [1006](#)
- création de cartes de données [1000](#)
- démarrage du cycle de journalisation du service de journalisation [998](#)
- mise à jour des propriétés du service d'écoute [1043](#)
- mise à jour des propriétés du service de journalisation [1046](#)
- mise à niveau des objets de données non relationnels [1041](#)

infacmd rms

- configuration des attributs de nœud de calcul [1067](#)
- configuration des propriétés du service du gestionnaire de ressource [1069](#)
- liste d'attributs de nœud de calcul [1064](#)
- liste des propriétés du service du gestionnaire de ressource [1066](#)

infacmd roh

- listProcessProperties [1052](#)
- listServiceOptions [1057](#)
- listServiceProcessOptions [1055](#)

infacmd rtm

- exportation des tables de référence [1074](#)
- importation de contenu depuis des fichiers d'application [1072](#)
- importation des tables de référence dans les référentiels modèles [1077](#)

infacmd sch

- création d'une planification [1080](#)
- mise à jour d'une planification [1095](#)
- suppression d'une planification [1087](#)

infacmd search

- configuration des propriétés pour le processus de service de recherche [1113](#)
- configuration des propriétés pour le service de recherche [1111](#)
- création de la liste de propriétés d'un processus de service de recherche [1110](#)
- création de la liste de propriétés pour le service de recherche [1108](#)
- création du service de recherche [1105](#)

infacmd sql

- actualisation du cache de la table virtuelle [1133](#)
- arrêt du service de données SQL [1148](#)
- changement de nom du service de données SQL [1134](#)
- configuration des autorisations du service de données SQL [1138](#)
- configuration des autorisations sur les colonnes de table virtuelle [1136](#)
- configuration des propriétés pour les tables virtuelles [1156](#)
- définition d'autorisations groupe et d'autorisations d'utilisateur sur les tables virtuelles [1143](#)
- définition des autorisations de l'utilisateur et du groupe des procédures stockées [1141](#)
- démarrage du service de données SQL [1146](#)
- liste des autorisations pour les colonnes virtuelles [1119](#)
- liste des autorisations pour un service de données SQL [1123](#)
- liste des propriétés des colonnes dans les tables virtuelles [1117](#)
- liste des propriétés des tables virtuelles [1127](#)
- liste des propriétés du service de données SQL [1121](#)

infacmd sql (a continué)

- liste des services de données SQL d'un service d'intégration de données [1124](#)
- liste les autorisations des tables virtuelles [1129](#)
- liste les autorisations pour les procédures stockées [1126](#)
- mise à jour des options du service de données SQL [1152](#)
- options de colonne [1152](#)
- options de la table virtuelle [1158](#)
- Options du service de données SQL [1154](#)
- purge du cache de la table virtuelle [1131](#)

infacmd tdm

- activation du service Test Data Manager. [1168](#)
- création d'un contenu de service Test Data Manager dans un domaine [1166](#)
- création d'un service Test Data Manager dans un domaine [1159](#)
- désactivation du service Test Data Manager [1169](#)

infacmd tools

- déploiement d'objets [1172](#)
- exportation de ressources vers les gestionnaire de métadonnées [1177](#)
- exportation des objets [1174](#)
- importation d'objets [1179](#)
- patchApplication [1185](#)

infacmd wfs

- abandon d'une instance de flux de travail [1188](#)
- achèvement d'une instance de tâche humaine [1194](#)
- annulation d'une instance de flux de travail [1192](#)
- création d'une liste d'instances de flux de travail actives [1201](#)
- création d'une liste de flux de travail dans une application [1211](#)
- création d'une liste de paramètres du flux de travail [1208](#)
- délégation d'une instance de tâche humaine [1198](#)
- démarrage d'une instance de flux de travail [1222](#)
- démarrage d'une tâche humaine dans un flux de travail [1221](#)
- libération d'une instance de tâche humaine [1216](#)
- liste de sorties de mappage persistantes [1203](#)
- Liste des instances de tâches humaines [1205](#)
- mise à jour de sorties de mappage persistantes [1218](#)
- omission des tables de base de données [1200](#)
- récupération d'une instance de flux de travail [1214](#)
- supprimer les données de processus de la base de données de flux de travail [1212](#)

infacmd ws

- création de la liste de propriétés pour une opération de service Web [1227](#)
- création de la liste des autorisations pour un service Web [1233](#)
- création de la liste des autorisations pour une opération de service Web [1229](#)
- ListOperationOptions [1227](#)
- ListOperationPermissions [1229](#)
- ListWebServiceOptions [1231](#)
- ListWebServicePermissions [1233](#)
- ListWebServices [1235](#)
- mettre à jour les propriétés d'un service Web [1249](#)
- mise à jour des propriétés d'une opération de service Web [1247](#)
- RenameWebService [1236](#)
- SetOperationPermissions [1238](#)
- SetWebServicePermissions [1241](#)
- StartWebService [1244](#)
- StopWebService [1246](#)
- UpdateOperationOptions [1247](#)
- UpdateWebServiceOptions [1249](#)

infacmd xrf

- génération de fichiers XML accessibles en lecture [1253](#)
- mise à jour de l'exportation XML [1254](#)

infasetup

- activer ou désactiver la complexité du mot de passe [1319](#)
- affichage des listes de suites de chiffres [1302](#)
- codes de retour [1274](#)

- infasetup (*a continué*)
 - domaine, mise à jour [1328](#)
 - domaines, définition [1278](#)
 - domaines, mise à jour [1311](#)
 - domaines, restauration [1303](#)
 - domaines, sauvegarde [1275](#)
 - domaines, suppression [1298](#)
 - exécuter [1274](#)
 - mise à jour des suites de chiffres [1308](#)
 - nœuds de calcul, définition [1294](#)
 - nœuds de passerelle, définition [1288](#)
 - nœuds de passerelle, mise à jour [788](#), [1311](#), [1329](#)
 - nœuds de travail, mise à jour [1323](#)
- INFATool_DATEFORMAT
 - configuration [60](#)
- Ingestion de masse
 - exécuter des statistiques [839](#)
- inscription
 - module de sécurité utilisant pmrep [1454](#)
 - plug-in utilisant pmrep [1453](#)
- Inscrire (pmrep)
 - description [1451](#)
- InstallAbapProgram (pmrep)
 - description [1425](#)
- Instances de tâches humaines [1194](#)
- instructions pour CI/CD
 - infacmd dis [278](#)

J

- journal de mappage
 - accès avec la commande infacmd ms [935](#)

L

- libellés
 - création à l'aide de pmrep [1406](#)
 - suppression [1414](#)
- licences
 - affichage de l'aide infacmd isp [716](#)
 - ajout aux domaines [368](#)
 - annulation de l'assignation à l'aide d'infacmd [728](#)
 - liste à l'aide d'infacmd isp [620](#)
 - liste de services assignés à [385](#)
 - mise à jour à l'aide d'infacmd isp [756](#)
 - retrait à l'aide d'infacmd isp [684](#)
- liens
 - ajout aux domaines [359](#)
- List (infacmd ps) [977](#)
- listActiveWorkflowInstances
 - infacmd wfs [1201](#)
- ListAlertUsers (infacmd isp)
 - description [581](#)
- listAllCustomLDAPTypes (infacmd isp)
 - description [583](#)
- ListAllGroups (infacmd isp)
 - description [584](#)
- listAllLDAPConnectivity (infacmd isp)
 - description [586](#)
- ListAllProfiles (infacmd ps) [979](#)
- ListAllRoles (infacmd isp)
 - description [587](#)
- ListAllUsers (infacmd isp)
 - description [589](#)
- ListAllUsers (pmrep)
 - description [1428](#)

- ListApplicationObjectPermissions (infacmd dis) [183](#)
- ListApplicationObjects (infacmd dis) [185](#)
- ListApplicationOptions (infacmd dis) [187](#)
- ListApplicationPermissions (infacmd dis) [189](#)
- ListApplications (infacmd dis) [190](#)
- listAssociatedConnections (grappe infacmd) [112](#)
- ListBackupFiles (infacmd mrs) [875](#)
- ListCheckedOutObjects (infacmd mrs) [876](#)
- listClusters (infacmd ccps) [97](#)
- ListColumnOptions (infacmd sql) [1117](#)
- ListComputeNodeAttributes (infacmd rms) [1064](#)
- ListComputeOptions (infacmd dis) [192](#), [254](#)
- listConfigurationGroupPermissions (cluster infacmd) [113](#)
- listConfigurationProperties (cluster infacmd) [116](#)
- listConfigurations (cluster infacmd) [118](#)
- listConfigurationSets (cluster infacmd) [115](#)
- listConfigurationUserPermissions (cluster infacmd) [120](#)
- ListConnectionOptions (infacmd isp)
 - description [590](#), [600](#)
- ListConnectionPermissionByUser (infacmd isp) [596](#)
- ListConnectionPermissions (infacmd isp) [592](#)
- ListConnectionPermissionsByGroup (infacmd isp)
 - description [594](#)
- ListConnections (infacmd isp)
 - description [598](#)
- ListConnections (pmrep)
 - description [1428](#)
- listCustomLDAPType (infacmd isp)
 - description [601](#)
- ListDataObjectOptions (infacmd dis) [193](#)
- ListDefaultOSProfiles (infacmd isp) [603](#)
- ListDomainLinks (infacmd isp)
 - description [607](#)
- ListDomainOptions (infacmd isp)
 - description [608](#)
- ListFolders (infacmd isp)
 - description [610](#)
- ListFOLDers (infacmd mrs) [878](#)
- listGlossary (infacmd bg) [89](#)
- ListGridNodes (infacmd isp)
 - description [611](#)
- ListGroupPermissions (infacmd isp) [613](#)
- ListGroupPrivileges (infacmd isp)
 - description [615](#)
- ListGroupsForUser (infacmd isp) [616](#)
- ListLicenses (infacmd isp)
 - description [620](#)
- ListLockedObjects (infacmd mrs) [880](#)
- listMappingEngines (infacmd dis) [195](#)
- listMappingEngines (infacmd mrs) [882](#)
- listMappingOptions (infacmd ms) [937](#)
- listMappingPersistedOutputs
 - infacmd wfs [1203](#)
- ListMappings (infacmd ms) [943](#)
- listMonitoringOptions (infacmd isp) [622](#)
- ListNodeOptions (infacmd isp)
 - description [623](#)
- ListNodeResources (infacmd isp)
 - description [625](#)
- ListNodeRoles (infacmd isp) [626](#)
- ListNodes (infacmd isp)
 - description [628](#)
- ListObjectDependencies (pmrep)
 - description [1428](#)
- ListObjects (pmrep)
 - description [1431](#)
 - liste des dossiers [1435](#)
 - types de transformation [1433](#)

- ListOperationOptions
 - infacmd ws [1227](#)
- ListOSProfiles (infacmd isp)
 - description [630](#)
- ListParameterSetObjects (infacmd dis) [200](#)
- ListParameterSets (infacmd dis) [201](#)
- listPatchNames
 - infacmd dis [203](#)
- listPermissionOnProject (infacmd mrs) [884](#)
- ListPlugins (infacmd) [65](#)
- listProcessProperties
 - infacmd roh [1052](#)
- ListProjects (infacmd mrs) [886](#)
- ListRepositoryLDAPConfiguration (infacmd isp)
 - description [632](#)
- ListRolePrivileges (infacmd isp)
 - description [633](#)
- ListSchedule (infacmd sch) [1088](#)
- ListSecurityDomains (infacmd)
 - description [635](#)
- ListSequenceObjectProperties (infacmd dis) [204](#)
- ListSequenceObjects (infacmd dis) [206](#)
- ListServiceLevels (infacmd isp)
 - description [636](#)
- ListServiceNodes (infacmd isp)
 - description [638](#)
- listServiceOptions
 - infacmd roh [1057](#)
- ListServiceOptions (infacmd as) [73](#)
- ListServiceOptions (infacmd cms) [136](#)
- ListServiceOptions (infacmd dis) [208](#)
- ListServiceOptions (infacmd mas) [821](#)
- ListServiceOptions (infacmd mrs) [888](#)
- ListServiceOptions (infacmd rms) [1066](#)
- ListServiceOptions (infacmd sch) [1090](#)
- ListServiceOptions (infacmd search) [1108](#)
- ListServicePrivileges (infacmd isp)
 - description [639](#)
- listServiceProcessOptions
 - infacmd roh [1055](#)
- ListServiceProcessOptions (infacmd as) [73](#)
- ListServiceProcessOptions (infacmd cms) [138](#)
- ListServiceProcessOptions (infacmd dis) [210](#)
- ListServiceProcessOptions (infacmd mas) [823](#)
- ListServiceProcessOptions (infacmd mrs) [889](#)
- ListServiceProcessOptions (infacmd sch) [1090](#)
- ListServiceProcessOptions (infacmd search) [1110](#)
- ListServices (infacmd isp)
 - description [641](#)
- ListSMTPOptions (infacmd isp) [643](#)
- listSpecs (infacmd mi) [843](#)
- ListSQLDataServiceOptions (infacmd sql) [1121](#)
- ListSQLDataServicePermissions (infacmd sql) [1123](#)
- ListSQLDataServices (infacmd sql) [1124](#)
- ListStoredProcedurePermissions (infacmd sql) [1126](#)
- ListTableOptions (infacmd sql) [1127](#)
- ListTablePermissions (infacmd sql) [1119](#), [1129](#)
- ListTablesBySess (pmrep)
 - description [1436](#)
- ListTaskListener (infacmd pwx) [1032](#)
- listTasks
 - infacmd wfs [1205](#)
- ListtLDAPConnectivity (infacmd isp)
 - description [618](#)
- ListUserConnections (pmrep)
 - description [1437](#)
- ListUserPermissions (infacmd isp) [645](#)

- ListUserPrivileges (infacmd isp)
 - description [647](#)
- ListWeakPasswordUsers (infacmd) [649](#)
- ListWebServiceOptions
 - infacmd ws [1231](#)
- ListWebServicePermissions
 - infacmd ws [1233](#)
- ListWebServices
 - infacmd ws [1235](#)
- listWorkflowParameters
 - infacmd wfs [1208](#)
- listWorkflows
 - infacmd wfs [1211](#)

M

- ManageGroupPermissionOnProject (infacmd mrs) [891](#)
- ManageUserPermissionOnProject (infacmd mrs) [893](#)
- mappage
 - configuration des autorisations pour [228](#)
- mappages
 - création de liste [937](#), [943](#)
- mappages déployés sur le service d'intégration de données
 - exécution [947](#)
- MassUpdate (pmrep)
 - description [1438](#)
- message électronique de post-session
 - mise à jour des adresses avec pmrep [1466](#)
- Microsoft SQL Server
 - syntaxe de chaîne de connexion [1383](#)
- MigrateEncryptionKey (infasetup)
 - description [1303](#)
- migrateProfileResults (infacmd ps) [980](#)
- migrateScorecards (infacmd ps) [982](#)
- migrateUsers
 - infacmd isp [650](#)
- Mise à niveau (infacmd cms) [150](#)
- mode attente
 - configuration à l'aide de pmcmd [1338](#)
- mode interactif pour pmcmd
 - connexion [1337](#)
 - paramètres par défaut [1337](#)
- mode ligne de commande pour pmcmd
 - connexion [1335](#)
- modèle de profil
 - annulation [962](#)
 - exécution [971](#)
 - obtention du statut [975](#)
- ModifyFolder (pmrep)
 - description [1444](#)
- modules de sécurité externe
 - désinscription [1463](#)
 - inscription [1454](#)
- mots de passe
 - chiffrement [61](#)
 - réinitialisation des mots de passe utilisateur à l'aide d'infacmd isp [707](#)
- MoveFolder (infacmd isp)
 - description [652](#)
- MoveObject (infacmd isp)
 - description [654](#)

N

- niveau d'optimisation
 - mise à jour [954](#), [956](#)

niveaux de service

- ajout [377](#)
- liste à l'aide d'infacmd isp [636](#)
- mise à jour à l'aide d'infacmd isp [781](#)
- retrait à l'aide d'infacmd isp [696](#)

nœud de calcul

- configuration des attributs [1067](#)
- liste d'attributs pour [1064](#)

nœuds

- ajout aux domaines [361](#)
 - ajout de ressources à [373](#)
 - basculement de passerelle à travail infacmd [721](#)
 - basculement de travail à passerelle infacmd [719](#)
 - définition d'un travail à l'aide de la commande infasetup [1294](#)
 - définition de la passerelle à l'aide de la commande infasetup [1288](#)
 - dissociation des domaines infacmd isp [735](#)
 - liste à l'aide d'infacmd isp [638](#)
 - liste de rôles [626](#)
 - liste de tous les nœuds dans un domaine [628](#)
 - liste des options à l'aide d'infacmd isp [623](#)
 - mise à jour [766](#)
 - mise à jour de la passerelle à l'aide de la commande infasetup [788](#), [1311](#), [1329](#)
 - mise à jour du nœud de travail à l'aide de la commande infasetup [1323](#)
 - mise à jour du rôle [768](#)
 - obtention du nom de [553](#)
 - ping [656](#)
 - retrait des domaines [686](#)
- nom du propriétaire de la table
- mise à jour avec pmrep [1468](#)
- Notify (pmrep)
- description [1446](#)

O

ObjectExport (pmrep)

- description [1446](#)

ObjectImport (pmrep)

- description [1448](#)

objet d'application

- configuration des autorisations pour [228](#)
- liste des autorisations des utilisateurs ou des groupes [183](#)

objets

- archivage [1395](#)
- attribution d'autorisations d'utilisateur sur [398](#)
- déploiement dans un fichier d'archive [1172](#)
- exportation [1446](#)
- exportation vers un fichier d'exportation d'objets [1174](#)
- importation [1448](#)
- importation depuis un fichier d'exportation d'objets [1179](#)
- retirer les autorisations d'utilisateur sur [700](#)
- suppression [1415](#)

objets de données

- configuration des propriétés pour [256](#)
- création de la liste de propriétés pour [193](#)

objets de données logiques

- options pour infacmd [258](#)
- purge du cache pour [211](#)

Objets du référentiel modèle

- exportation [342](#)
- objet de rapport, réutilisation [348](#)

opérateurs de comparaison

- chemin de dossier [282](#)
- requête [281](#)

opérateurs logiques

- requête [283](#)

opération de service Web

- création de la liste de propriétés pour [1227](#)
- création de la liste des autorisations pour [1229](#)
- mise à jour des propriétés pour [1247](#)
- paramétrage des autorisations avec la commande infacmd [1238](#)
- options de colonne virtuelle infacmd sqlupdate [1150](#)
- options de connexion
 - DB2 for infacmd [438](#)
 - SEQ pour infacmd [468](#)
 - VSAM pour infacmd [476](#)
- options de mappage
 - mise à jour [952](#)
- Options de surveillance du domaine de la commande infacmd isp list [622](#)
- Options de surveillance du domaine de la commande infacmd isp update [760](#)
- Options du service d'accès aux métadonnées
 - syntaxe infacmd [827](#)
- Options du service d'intégration de données
 - syntaxe infacmd [263](#)
- Options du service de planificateur
 - syntaxe infacmd [1100](#), [1102](#)
- Options du service du gestionnaire de ressource
 - syntaxe infacmd [1071](#)
- options du service Web
 - syntaxe infacmd [1251](#)
- Oracle
 - options de connexion pour [462](#)
 - syntaxe de chaîne de connexion [1383](#)
- OVERIDEFOLDER
 - exemple de fichier de contrôle [1508](#)

P

paramètres de requête

- requête [283](#)

passerelle

- mise à jour des informations à l'aide d'infacmd isp [748](#)

PauseAll (infacmd sch) [1092](#)

PauseSchedule (infacmd sch) [1092](#)

ping

- domaine [657](#)
- nœud [657](#)
- service [657](#)

Ping (infacmd isp)

- description [656](#)

pingservice (pmcmd)

- description [1358](#)

plug-ins

- modèles XML [1454](#)

pmcmd

- codes de retour [1336](#)
- dossiers, désignation d'aucun dossier par défaut [1375](#)
- dossiers, désignation pour l'exécution des commandes [1362](#)
- exécuté dans un domaine multiversions [1335](#)
- fichiers de paramètres [1366](#), [1369](#)
- fichiers script [1338](#)
- flux de travail, abandon [1342](#)
- flux de travail, arrêt [1372](#)
- flux de travail, démarrage [1367](#)
- flux de travail, indication de fonctionnement [1378](#)
- flux de travail, obtention de détails [1347](#), [1354](#)
- flux de travail, planification [1361](#)
- flux de travail, récupération [1359](#)
- flux de travail, suppression dans un planificateur [1374](#)
- mode attente, configuration [1363](#)
- mode interactif [1337](#)

pmcmd (a continué)

- mode interactif, fermeture [1345](#)
- mode ligne de commande [1335](#)
- mode nowait, configuration [1363](#)
- paramètres du service, obtention [1363](#)
- Service d'intégration de PowerCenter, obtention de propriétés [1349](#)
- Service d'intégration, connexion [1344](#)
- Service d'intégration, déconnexion [1345](#)
- Service d'intégration, ping [1358](#)
- sessions, obtention de détails [1346](#)
- statistiques de session, obtention [1350](#)
- tâches, abandon [1340](#)
- tâches, arrêt [1370](#)
- tâches, démarrage [1364](#)
- tâches, finalisation avant le retour à l'invite [1376](#)
- tâches, obtention de détails [1347](#), [1352](#)
- version, affichage [1376](#)

pmpasswd

- chiffrement des mots de passe [61](#)
- syntaxe [61](#)

pmrep

- adresses électroniques, mise à jour [1466](#)
- aide [1425](#)
- autorisation, assignation [1392](#)
- connexions utilisateur, liste [1437](#)
- connexions utilisateur, mise en arrêt [1427](#)
- connexions, création [1400](#)
- connexions, liste [1428](#)
- connexions, mise à jour [1464](#)
- connexions, suppression [1413](#)
- dépendances d'objet, liste [1428](#)
- déploiement, annulation [1456](#)
- désinstallez le programme ABAP [1471](#)
- détails de connexion, liste [1423](#)
- dossiers, création [1404](#)
- dossiers, déploiement [1418](#)
- dossiers, liste [1435](#)
- dossiers, modification des propriétés [1444](#)
- dossiers, suppression [1414](#)
- exécuté dans un domaine multiversions [1382](#)
- extractions, annulation [1460](#)
- fichier de connexion du référentiel, spécification [58](#)
- fichiers d'entrée persistants, création [1488](#)
- fichiers script [1384](#)
- génération du programme ABAP [1423](#)
- groupes de déploiement, ajout d'objets [1387](#)
- groupes de déploiement, création [1403](#)
- groupes de déploiement, déploiement [1416](#)
- groupes de déploiement, effacement d'objets [1396](#)
- groupes de déploiement, suppression [1414](#)
- groupes, création [1406](#)
- informations de connexion, affichage [1458](#)
- informations de version, affichage [1475](#)
- installation du programme ABAP [1425](#)
- journaux, suppression [1459](#)
- libellés, application [1389](#)
- libellés, création [1406](#)
- libellés, suppression [1414](#)
- mode interactif [1382](#)
- mode interactif, fermeture [1421](#)
- mode interactif, quitter [1421](#)
- mode ligne de commande [1382](#)
- nom de connexion, modification [1459](#)
- noms des propriétaires de la table, mise à jour [1468](#)
- notification de messages, envoi [1446](#)
- objets extraits, liste [1421](#)
- objets, archivage [1395](#)
- objets, changement de propriété [1394](#)

pmrep (a continué)

- objets, exportation [1446](#)
- objets, importation [1448](#)
- objets, liste [1431](#)
- objets, suppression [1415](#)
- objets, validation [1473](#)
- paramètres de contrôle de l'importation d'objets [1491](#)
- paramètres du fichier de contrôle de déploiement [1503](#)
- plug-ins, désinscription [1462](#)
- plug-ins, inscription [1453](#)
- préfixes du nom de table cible, mise à jour [1470](#)
- présentation [1382](#)
- privileges, suppression [1456](#)
- propriétés de dossier, modification [1444](#)
- propriétés utilisateur, édition [1419](#)
- référentiels, connexion [1397](#)
- référentiels, création [1399](#)
- référentiels, désinscription [1461](#)
- référentiels, inscription [1451](#)
- référentiels, restauration [1455](#)
- référentiels, sauvegarde [1393](#)
- référentiels, suppression [1412](#)
- requêtes, exécution [1419](#)
- ressources, nettoyage [1396](#)
- scripts, exécution [1457](#)
- service d'intégration PowerCenter, attribution [1391](#)
- statistiques du référentiel, mise à jour [1469](#)
- tables, liste par session [1436](#)
- utilisateurs, listes [1428](#)
- valeurs de séquence, mise à jour [1467](#)
- versions d'objet, purge [1449](#)
- PopulateVCS (infacmd mrs) [895](#)
- PrintSPNAndKeytabNames (infacmd isp) [659](#)
- privileges
 - assignation aux groupes dans un domaine [363](#)
 - assignation aux rôles [375](#)
 - liste des services à l'aide d'infacmd isp [639](#)
 - liste pour un groupe à l'aide d'infacmd isp [615](#)
 - liste pour un rôle à l'aide d'infacmd isp [633](#)
 - liste pour un utilisateur [647](#)
 - retrait [1456](#)
 - retrait d'un groupe à l'aide d'infacmd isp [680](#)
 - retrait d'un rôle à l'aide d'infacmd isp [692](#)
 - retrait d'un utilisateur à l'aide d'infacmd isp [703](#)
- procédures stockées
 - configuration des autorisations pour [1141](#)
 - création de la liste des autorisations pour [1126](#)
- processus de service
 - activation sur les nœuds [537](#)
 - désactivation sur un nœud [527](#)
- Processus de service Analyst
 - configuration des propriétés pour [75](#)
- processus de service d'accès aux métadonnées
 - liste des propriétés de [823](#)
- Processus de service d'accès aux métadonnées
 - configuration des propriétés du [828](#)
- processus de service d'application
 - obtention du statut pour [560](#)
- Processus de service d'intégration
 - mise à jour des options pour [782](#)
 - obtention des propriétés pour [558](#)
- Processus de service de gestion du contenu
 - configuration des options pour [148](#)
- processus de service de recherche
 - configuration des propriétés pour [1113](#)
 - création de la liste de propriétés pour [1110](#)
- processus du service d'intégration de données
 - configuration des propriétés pour [275](#)

- processus du service d'intégration de données (*a continué*)
 - création de la liste de propriétés pour [210](#)
 - liste des propriétés [204](#)
- profil de système d'exploitation
 - attribution de profil par défaut à un utilisateur ou à un groupe [383](#)
 - liste des profils par défaut [603](#)
 - mise à jour à l'aide d'infacmd isp [771](#)
 - suppression du profil par défaut d'un utilisateur ou d'un groupe [725](#)
- profil du processeur
 - calcul à l'aide d'infacmd isp [709](#)
- profil du système d'exploitation
 - liste à l'aide d'infacmd isp [630](#)
 - retrait à l'aide d'infacmd isp [689](#)
- profils
 - détection de résultats pour [966](#)
 - exécution [969](#)
 - liste les résultats de [977](#)
 - purge les résultats de [984](#)
 - tables de détection pour [986](#)
- profils de système d'exploitation
 - création dans un domaine [498](#)
- programmes de ligne de commande
 - présentation [36](#)
 - syntaxe pour [38](#)
- pruneOldInstances
 - infacmd wfs [1212](#)
- Purge (infacmd cms) [139](#)
- Purge (infacmd ps) [984](#)
- purge des tâches du service d'intégration de données [945](#)
- purgeauditevents (infacmd edp) [307](#)
- purgeDatabaseWorkTabless (infacmd dm) [945](#)
- PurgeDataObjectCache (infacmd dis) [211](#)
- PurgeLog (infacmd isp)
 - description [660](#)
- purgeOrphanResults (infacmd ps) [986](#)
- PurgeResultSetCache (infacmd dis) [213](#)
- PurgeTableCache (infacmd sql) [1131](#)
- PurgeVersion (pmrep)
 - description [1449](#)

Q

- queryDesignTimeObjects
 - infacmd dis [215](#)
- queryRunTimeObjects
 - infacmd dis [217](#)

R

- reassignCheckedOutObject (infacmd mrs) [896](#)
- rebuildDependencyGraph (infacmd mrs) [898](#)
- recoverWorkflow
 - infacmd wfs [1214](#)
- recoverworkflow (pmcmd)
 - description [1359](#)
- récupérer les journaux de cluster agrégés
 - infacmd ms [931](#)
- référentiel modèle
 - régénération du graphique de dépendance d'objet [898](#)
- Référentiel modèle
 - archivage d'objets dans [853](#)
 - déverrouillage d'un objet dans [911](#)
 - Dresse la liste des options du service de référentiel modèle [888](#)
 - Liste de dossiers dans le référentiel du service de référentiel modèle [878](#)
 - Liste des autorisations dans plusieurs projets [884](#)

- Référentiel modèle (*a continué*)
 - Liste des fichiers du dossier de sauvegarde [875](#)
 - liste des objets extraits dans [876](#)
 - liste des objets verrouillés dans [880](#)
 - Liste des projets dans le référentiel du service de référentiel modèle [886](#)
 - Met à jour les options du processus de service pour le Service de Référentiel Modèle [920](#)
 - Met à jour les options du service de référentiel modèle [913](#)
 - Met à jour les statistiques du service de référentiel modèle [921](#)
 - mise à niveau du Service de Référentiel Modèle [923](#)
 - réattribution de l'objet extrait dans [896](#)
 - réattribution de l'objet verrouillé dans [896](#)
 - restauration du contenu de [903](#)
 - rétablissement d'objets extraits dans [905](#), [909](#)
 - sauvegarde du contenu dans un fichier [851](#)
 - suppression du contenu de [864](#)
- référentiels
 - connexion à l'aide de pmrep [1397](#)
 - création de relationnel [1400](#)
 - désinscription [1461](#)
 - inscription [1451](#)
 - sauvegarde à l'aide de pmrep [1393](#)
 - suppression des détails de [1459](#)
- refreshConfiguration (cluster infacmd) [121](#)
- RefreshDataObjectCache (infacmd dis) [218](#)
- RefreshTableCache (infacmd sql) [1133](#)
- RegisterPlugin (pmrep)
 - description [1453](#)
- releaseTask
 - infacmd wfs [1216](#)
- RemoveAlertUser (infacmd isp)
 - description [664](#)
- RemoveConnection (infacmd isp)
 - description [666](#)
- RemoveConnectionPermissions (infacmd isp)
 - description [668](#)
- removeCustomLDAPType (infacmd isp)
 - description [670](#)
- RemoveDomainLink (infacmd isp)
 - description [672](#)
- RemoveFolder (infacmd isp)
 - description [674](#)
- RemoveGrid (infacmd isp)
 - description [675](#)
- RemoveGroup (infacmd isp)
 - description [677](#)
- RemoveGroupPermission (infacmd isp) [678](#)
- RemoveGroupPrivilege (infacmd isp)
 - description [680](#)
- removeLDAPConnectivity (infacmd isp)
 - description [682](#)
- RemoveLicense (infacmd isp)
 - description [684](#)
- RemoveNode (infacmd isp)
 - description [686](#)
- RemoveNodeResource (infacmd isp)
 - description [687](#)
- RemoveOSProfile (infacmd isp)
 - description [689](#)
- RemoveRole (infacmd isp)
 - description [691](#)
- RemoveRolePrivilege (infacmd isp)
 - description [692](#)
- RemoveService (infacmd cms) [141](#)
- RemoveService (infacmd isp)
 - description [694](#)

- RemoveServiceLevel (infacmd isp)
 - description [696](#)
- RemoveUser (infacmd isp)
 - description [697](#)
- RemoveUserFromGroup (infacmd isp)
 - description [699](#)
- RemoveUserPermission (infacmd isp) [700](#)
- RemoveUserPrivilege (infacmd isp)
 - description [703](#)
- RenameApplication (infacmd dis) [220](#)
- RenameConnection (infacmd isp) [705](#)
- RenameFolder (infacmd mrs) [900](#)
- RenameSQLDataService (infacmd sql) [1134](#)
- RenameWebService
 - infacmd ws [1236](#)
- replaceAllTag
 - infacmd dis [246](#)
- requête
 - clause Where [286](#)
 - infacmd dis [280](#)
 - opérateurs de comparaison [281](#)
 - opérateurs logiques [283](#)
 - paramètres de requête [283](#)
 - structure de requête [285](#)
- requêtes
 - exécution [1419](#)
- ResetPassword (infacmd isp)
 - description [707](#)
- ressources
 - affichage à l'aide d'infacmd isp [625](#)
 - exportation vers un fichier d'exportation d'objets [1177](#)
 - retrait à l'aide d'infacmd isp [687](#)
- Ressources PowerCenter
 - activation [534](#)
 - désactivation [523](#)
- restartMapping (infacmd mi) [844](#)
- restauration
 - référentiels à l'aide de pmrep Restore [1455](#)
- Restore (pmrep)
 - description [1455](#)
- RestoreApplication (infacmd dis) [224](#)
- RestoreContents (infacmd mrs) [903](#)
- RestoreDomain (infasetup)
 - description [1303](#)
- restoreMitKerberosLinkage (infasetup)
 - description [1306](#)
- ResumeAll (infacmd sch) [1093](#)
- ResumeSchedule (infacmd sch) [1094](#)
- resyncData (infacmd cms) [143](#)
- RevertObject (infacmd mrs) [905](#), [909](#)
- revive_Scorecards (infacmd ps) [988](#)
- RmPrivilege (pmrep)
 - description [1456](#)
- rôles
 - assignation à un utilisateur à l'aide d'infacmd isp [394](#)
 - création dans un domaine [509](#)
 - exportation à l'aide d'infacmd isp [541](#)
 - importation à l'aide d'infacmd isp [574](#)
 - liste à l'aide d'infacmd isp [587](#)
 - retrait à l'aide d'infacmd isp [691](#)
 - retrait d'un groupe à l'aide d'infacmd isp [730](#)
 - retrait d'un utilisateur à l'aide d'infacmd isp [731](#)
- RollbackDeployment (pmrep)
 - description [1456](#)
- Run (pmrep)
 - description [1457](#)
- RunCPUProfile (infacmd isp)
 - description [709](#)

- RunMapping
 - infacmd ms [947](#)
- runSpec
 - infacmd mi [845](#)

S

- Sauvegarde (pmrep)
 - description [1393](#)
- scheduleworkflow (pmcmd)
 - description [1361](#)
- schémas virtuels
 - création de la liste des autorisations pour [1117](#)
- SEQ
 - options de connexion infacmd [468](#)
- Service Analyst
 - création dans un domaine [70](#)
 - création de la liste de propriétés pour [73](#)
 - création de tables d'audit pour les tâches de gestion des exceptions [68](#)
 - exporter les glossaires d'entreprise [90](#)
 - importation de glossaires d'entreprise à partir de fichiers .xlsx [92](#)
 - liste de configuration pour [73](#)
 - liste des glossaires d'entreprise [89](#)
 - mise à jour des propriétés pour [74](#)
 - mise à niveau de données de Business Glossary [87](#)
 - suppression de tables d'audit pour les tâches de gestion des exceptions [72](#)
 - supprimer l'historique de l'audit du glossaire d'entreprise [88](#)
- service Blaze
 - arrêt [238](#)
- Service d'accès aux métadonnées
 - configuration des propriétés du [825](#)
 - création [817](#)
 - liste des propriétés de [821](#)
- service d'écoute PowerExchange
 - affichage des statistiques de surveillance pour le service d'écoute et ses tâches [1024](#)
 - arrêt [995](#)
 - arrêt des tâches [1038](#)
 - arrêt forcé [993](#)
 - création [1003](#)
 - liste des tâches [1032](#)
 - mise à jour des propriétés [1043](#)
- Service d'ingestion de masse
 - Création [833](#)
- Service d'intégration
 - assignation au service de gestionnaire de métadonnées [388](#)
 - création [484](#)
 - mise à jour à l'aide d'infacmd isp [751](#)
 - retrait à l'aide d'infacmd isp [694](#)
- Service d'intégration de données
 - configuration des propriétés [261](#)
 - configuration des propriétés de calcul [254](#)
 - création [159](#)
 - création de la liste de propriétés pour [208](#)
 - liste [195](#)
 - liste des propriétés de calcul [192](#)
- service d'intégration PowerCenter
 - attribution à l'aide de pmrep [1391](#)
- Service de données SQL
 - arrêt [1148](#)
 - changement de nom [1134](#)
 - configuration des autorisations pour [1138](#)
 - création de la liste de propriétés pour [1121](#)
 - création de la liste des autorisations pour [1123](#)
 - démarrage [1146](#)

Service de données SQL (*a continué*)
 liste pour un service d'intégration de données [1124](#)
 mise à jour des options pour [1152](#)
 options pour infacmd [1154](#)

Service de flux de travail
 omission des tables de base de données [1200](#)

Service de gestion de contenu
 création dans un domaine [132](#)
 mise à jour des options pour [145](#)
 synchronisation des données avec l'ordinateur CMS principal [143](#)

Service de gestion du contenu
 création d'une liste d'options pour [138](#)
 création de la liste de propriétés pour [136](#)
 Mise à niveau [150](#)
 purge des données de référence orphelines [139](#)
 suppression à l'aide infacmd cms [141](#)

Service de journalisation PowerExchange
 affichage de l'état de la sous-tâche du dispositif d'écriture [1027](#)
 affichage de l'utilisation de la mémoire [1018](#)
 affichage de tous les messages [1010](#)
 affichage des événements [1015](#)
 affichage des informations CPU [1013](#)
 affichage du nombre d'enregistrements de modifications traités [1021](#)
 basculement à un nouvel ensemble de fichiers journaux [1030](#)
 création [1006](#)
 démarrage de cycle de journalisation [998](#)
 fermeture [1035](#)
 mise à jour des propriétés [1046](#)

service de préparation de données interactive
 création [293](#)
 mise à jour [297](#)

Service de recherche
 configuration des propriétés pour [1111](#)
 création [1105](#)
 création de la liste de propriétés pour [1108](#)

Service de référentiel
 création dans un domaine [504](#)
 mise à jour à l'aide d'infacmd isp [774](#)
 retrait à l'aide d'infacmd isp [694](#)

Service de référentiel modèle
 création [860](#)
 création du contenu du référentiel pour [855](#)
 liste [882](#), [889](#)

Service du gestionnaire de ressource
 configuration des propriétés du [1069](#)
 liste des propriétés de [1066](#)

service Enterprise Data Preparation
 mise à jour [310](#)
 mise à niveau [313](#)
 purge audit events [307](#)

Service Enterprise Data Preparation
 création [303](#)

Service Metadata Manager
 création dans un domaine [494](#)
 mise à jour des propriétés pour [758](#)

Service SAP BW
 création dans un domaine [510](#)
 mise à jour à l'aide d'infacmd isp [779](#)

Service TDM
 désactivation [1169](#)

Service Test Data Manager
 création dans un domaine [1159](#), [1166](#)

service web
 arrêt à l'aide de la commande infacmd [1246](#)
 création d'une liste avec la commande infacmd [1235](#)
 création de la liste de propriétés pour [1231](#)
 création de la liste des autorisations pour [1233](#)

service web (*a continué*)
 démarrage avec la commande infacmd [1244](#)
 mise à jour des propriétés pour [1249](#)
 modification d'un nom avec la commande infacmd [1236](#)
 paramétrage des autorisations avec la commande infacmd [1241](#)

services
 liste à l'aide d'infacmd isp [641](#)
 ping [656](#)

services d'application
 désactivation [525](#)

services d'applications
 activation [535](#), [1168](#)
 obtention des propriétés pour [557](#)
 obtention du statut pour [562](#)
 retrait à l'aide d'infacmd isp [694](#)

sessions
 obtention d'événements du journal pour [563](#)

SetApplicationObjectPermissions (infacmd dis) [228](#)

SetApplicationPermissions (infacmd dis) [226](#)

SetColumnPermissions (infacmd sql) [1136](#)

SetComputeNodeAttributes (infacmd rms) [1067](#)

setConfigurationPermissions (cluster infacmd) [123](#)

SetConnectionPermissions (infacmd isp) [711](#)

SetFolder (pmcmd)
 description [1362](#)

setMappingPersistedOutputs
 infacmd wfs [1218](#)

SetNoWait (pmcmd)
 description [1363](#)

SetOperationPermissions
 infacmd ws [1238](#)

SetRepositoryLDAPConfiguration (infacmd isp)
 description [713](#)

SetSequenceState (infacmd dis) [232](#)

SetSQLDataServicePermissions (infacmd sql) [1138](#)

SetStoredProcedurePermissions (infacmd sql) [1141](#)

SetTablePermissions (infacmd sql) [1143](#)

SetWait (pmcmd)
 description [1363](#)

SetWebServicePermissions
 infacmd ws [1241](#)

ShowConnectionInfo (pmrep)
 description [1458](#)

ShowLicense (infacmd isp)
 description [716](#)

ShowSettings (pmcmd)
 description [1363](#)

ShutDownLogger (infacmd pwx) [1035](#)

ShutdownNode (infacmd isp)
 description [717](#)

sorties de mappage
 mise à jour avec la commande infacmd [1218](#)

sorties de mappage persistantes
 suppression avec la commande infacmd ms [929](#)

Spéc
 déploiement dans un fichier d'archive [838](#)

spécification d'ingestion de masse
 abandon [831](#)

spécifications déployées dans un service d'intégration de données
 exécution [845](#)

StartApplication (infacmd dis) [235](#)

StartSQLDataService (infacmd sql) [1146](#)

startTask
 infacmd wfs [1221](#)

StartTask (pmcmd)
 description [1364](#)
 utilisation d'un fichier de paramètres [1366](#)

- StartWebService
 - infacmd ws [1244](#)
- startWorkflow
 - infacmd wfs [1222](#)
- StartWorkflow (pmcmd)
 - description [1367](#)
 - utilisation d'un fichier de paramètres [1369](#)
- statistiques
 - mise à jour du référentiel [1469](#)
- statut de mappage
 - accès avec la commande infacmd ms [933](#)
- statut de spéc
 - accès avec infacmd mi [841](#)
- StopApplication (infacmd dis) [236](#)
- stopBlazeService (infacmd dis) [238](#)
- StopSQLDataService (infacmd sql) [1148](#)
- StopTask (pmcmd)
 - description [1370](#)
- StopTaskListener (infacmd pwx) [1038](#)
- StopWebService
 - infacmd ws [1246](#)
- StopWorkflow (pmcmd)
 - description [1372](#)
- structure de requête
 - requête [285](#)
- surveillance de domaine
 - liste d'options [622](#)
 - options de mise à jour [760](#)
- SwitchConnection (pmrep)
 - description [1459](#)
- SwitchToGatewayNode (infacmd)
 - description [719](#)
- SwitchToKerberosMode (infasetup)
 - description [1307](#)
- SwitchToWorkerNode (infacmd isp)
 - description [721](#)
- synchronizeProfile (infacmd ps) [990](#)
- SyncSecurityDomains (infacmd isp) [723](#)
- syntaxe
 - Options infacmd du service d'accès aux métadonnées [827](#)
 - Options infacmd du service d'intégration de données [263](#)
 - Options infacmd du service de planificateur [1100](#), [1102](#)
 - Options infacmd du service du gestionnaire de ressource [1071](#)
 - programmes de ligne de commande [38](#)

T

- tables de référence
 - exportation [1074](#)
 - importation dans les référentiels modèles [1077](#)
- tables de suivi d'audit
 - service de gestion du contenu, création [130](#)
 - Suppression du service de gestion du contenu [134](#)
- tables virtuelles
 - configuration des autorisations pour [1143](#)
 - configuration des propriétés pour [1156](#)
 - création de la liste de propriétés pour [1127](#)
 - création de la liste des autorisations pour [1129](#)
 - options pour infacmd [1158](#)
- tâches
 - abandon [927](#)
 - purge [945](#)
- tâches de profil
 - obtention du statut [990](#)
- Tâches de profil
 - Obtention du statut [973](#)

- tag
 - infacmd dis [241](#)
- TruncateLog (pmrep)
 - description [1459](#)

U

- UnassignDefaultOSProfile (infacmd isp) [725](#)
- UnassignSMMSservice (infacmd)
 - description [726](#)
- UnassignLicense (infacmd)
 - description [728](#)
- UnassignRoleFromGroup (infacmd isp)
 - description [730](#)
- UnassignRoleFromUser (infacmd isp)
 - description [731](#)
- UnassignRSWSHubService (infacmd isp)
 - description [734](#)
- UnassociateDomainNode (infacmd isp)
 - description [735](#)
- UndeployApplication (infacmd dis) [249](#)
- UndoCheckout (pmrep)
 - description [1460](#)
- UninstallAbapProgram (pmrep)
 - description [1471](#)
- unlockObject (infacmd mrs) [911](#)
- Unregister (pmrep)
 - description [1461](#)
- UnregisterPlugin (pmrep)
 - description [1462](#)
- UnscheduleWorkflow (pmcmd)
 - description [1374](#)
- UnsetFolder (pmcmd)
 - description [1375](#)
- untag
 - infacmd dis [243](#)
- updateADLSCertificate (infacmd ccps) [99](#)
- UpdateApplication (infacmd dis) [250](#)
- UpdateApplicationOptions (infacmd dis) [252](#)
- UpdateColumnOptions (infacmd sql) [1150](#)
- updateConfiguration (cluster infacmd) [127](#)
- UpdateConnection (infacmd isp)
 - description [737](#)
- UpdateConnection (pmrep)
 - description [1464](#)
- updateCustomLDAPType (infacmd isp)
 - description [741](#)
- UpdateDataObjectsOptions (infacmd dis) [256](#)
- updateDomainName (infasetup)
 - description [1311](#)
- UpdateDomainOptions (infacmd isp)
 - description [744](#)
- updateDomainSamlConfig (infasetup)
 - description [1320](#)
- UpdateEmailAddr (pmrep)
 - description [1466](#)
- updateExportXML
 - infacmd xrf [1254](#)
- UpdateFolder (infacmd isp)
 - description [746](#)
- UpdateGatewayInfo (infacmd isp)
 - description [748](#)
- UpdateGatewayNode (infasetup)
 - description [1311](#)
- UpdateGrid (infacmd isp)
 - description [749](#)

- UpdateIntegrationService (infacmd isp)
 - description [751](#)
- UpdateKerberosAdminUser (infasetup)
 - description [1317](#)
- UpdateKerberosConfig (infasetup)
 - description [1317](#)
- updateLDAPConnectivity (infacmd isp)
 - description [753](#)
- UpdateLicense (infacmd isp)
 - description [756](#)
- UpdateListenerService (infacmd pwx) [1043](#)
- UpdateLoggerService (infacmd pwx) [1046](#)
- updateMappingOptions (infacmd ms) [952](#)
- updateMitKerberosLinkage (infasetup)
 - description [1318](#)
- UpdateMMService (infacmd isp)
 - description [758](#)
- UpdateMonitoringOptions (infacmd isp) [760](#)
- UpdateNamespace (infacmd isp) [763](#)
- UpdateNodeOptions (infacmd isp)
 - description [766](#)
- UpdateNodeRole (infacmd isp) [768](#)
- UpdateOperationOptions
 - infacmd ws [1247](#)
- updateOptimizationDefaultLevel (infacmd ms) [954](#)
- updateOptimizationLevel (infacmd ms) [956](#)
- UpdateOSProfile (infacmd isp)
 - description [771](#)
- UpdateParameterSetEntries (infacmd dis) [259](#)
- UpdatePasswordComplexityConfig (infasetup) [1319](#)
- UpdateRepositoryService (infacmd isp)
 - description [774](#)
- updateSamlConfig (infasetup)
 - description [1320](#)
- UpdateSAPBWSservice (infacmd isp)
 - description [779](#)
- UpdateSchedule (infacmd sch) [1095](#)
- UpdateSeqGenVals (pmrep)
 - description [1467](#)
- updateService (infacmd edp) [310](#)
- updateService (infacmd idp) [297](#)
- UpdateServiceLevel (infacmd isp)
 - description [781](#)
- UpdateServiceOptions (infacmd as) [74](#)
- UpdateServiceOptions (infacmd cms) [145](#)
- UpdateServiceOptions (infacmd dis) [261](#), [913](#)
- UpdateServiceOptions (infacmd mas) [825](#)
- UpdateServiceOptions (infacmd rms) [1069](#)
- UpdateServiceOptions (infacmd sch) [1098](#)
- UpdateServiceOptions (infacmd search) [1111](#)
- UpdateServiceProcess (infacmd isp)
 - description [782](#)
- UpdateServiceProcessOptions (infacmd as) [75](#)
- UpdateServiceProcessOptions (infacmd cms) [148](#)
- UpdateServiceProcessOptions (infacmd dis) [275](#)
- UpdateServiceProcessOptions (infacmd mas) [828](#)
- UpdateServiceProcessOptions (infacmd mrs) [920](#)
- UpdateServiceProcessOptions (infacmd sch) [1101](#)
- UpdateServiceProcessOptions (infacmd search) [1113](#)
- UpdateSMTPOptions (infacmd isp)
 - description [784](#)
- UpdateSQLDataServiceOptions (infacmd sql) [1152](#)
- UpdateSrcPrefix (pmrep)
 - description [1468](#)
 - mise à jour de sessions non réutilisables [1468](#)
- updateStatistics (infacmd mrs) [921](#)
- UpdateStatistics (pmrep)
 - description [1469](#)

- UpdateTableOptions (infacmd sql) [1156](#)
- UpdateTargPrefix (pmrep)
 - description [1470](#)
 - mise à jour de sessions non réutilisables [1470](#)
- UpdateWebServiceOptions
 - infacmd ws [1249](#)
- UpdateWorkerNode (infasetup)
 - description [1323](#)
- UpdateWSHubService (infacmd isp)
 - description [786](#)
- Upgrade (infacmd sch) [1103](#)
- UpgradeContents (infacmd mrs) [923](#)
- upgradeDomainMetadata
 - description [1328](#)
- UpgradeGatewayNodeMetadata (infasetup)
 - description [788](#), [1329](#)
- UpgradeModels (infacmd pwx) [1041](#)
- upgradeRepository (infacmd bg) [87](#)
- upgradeService (infacmd edp) [313](#)
- URL du fournisseur d'identité
 - définition [1320](#)
 - obtention [555](#)
- utilisateurs
 - ajout au groupe dans un domaine [381](#)
 - création dans un domaine [514](#)
 - exportation [544](#)
 - exportation à l'aide d'infacmd isp [541](#)
 - importation à l'aide d'infacmd isp [574](#), [579](#)
 - liste à l'aide d'infacmd isp [589](#)
 - liste de types d'autorisations pour [596](#)
 - migration avec la commande infacmd [650](#)
 - répertoire des groupes pour un utilisateur [616](#)
 - retrait à l'aide d'infacmd isp [697](#)
 - retrait d'un groupe à l'aide d'infacmd isp [699](#)
- utilisateurs et groupes
 - retrait des autorisations pour [711](#)
- utilisateurs et groupes dans le domaine de sécurité
 - synchronisation avec les utilisateurs et les groupes LDAP [723](#)
- utilitaires de ligne de commande
 - configuration [33](#)
 - fichier domains.infa [34](#)
- utilitaires de ligne de commande (configurer les utilitaires Metadata Manager) [34](#)
- utilitaires de ligne de commande (configurer les utilitaires PowerCenter) [33](#)
- utilitaires Informatica (configuration de sécurité) [35](#)
- utilitaires Informatica (installation) [32](#)
- utilitaires Metadata Manager
 - configuration [34](#)
 - configuration de sécurité [35](#)
 - installation [32](#)
- utilitaires PowerCenter
 - configuration [33](#)
 - configuration de sécurité [35](#)
 - installation [32](#)

V

- Validate (pmrep)
 - description [1473](#)
- ValidateandRegisterFeature (infasetup)
 - description [1332](#)
- validateFeature (infacmd advanced) [790](#)
- validation des objets
 - avec pmrep [1473](#)
- variables d'environnement
 - configuration pour les programmes de ligne de commande [44](#)

variables d'environnement (*a continué*)

ICMD_JAVA_OPTS [46](#)
INFA_CLIENT_RESILIENCE_TIMEOUT [46](#)
INFA_CODEPAGENAME [47](#)
INFA_DEFAULT_DATABASE_PASSWORD [48](#)
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](#)

Version (infacmd)

description [792](#)

Version (pmcmd)

description [1376](#)

Version (pmrep)

description [1475](#)

VSAM

options de connexion infacmd [476](#)

W

WaitTask (pmcmd)

description [1376](#)

WaitWorkflow (pmcmd)

description [1378](#)

Web Content-Kapow Catalyst

connexion [478](#)